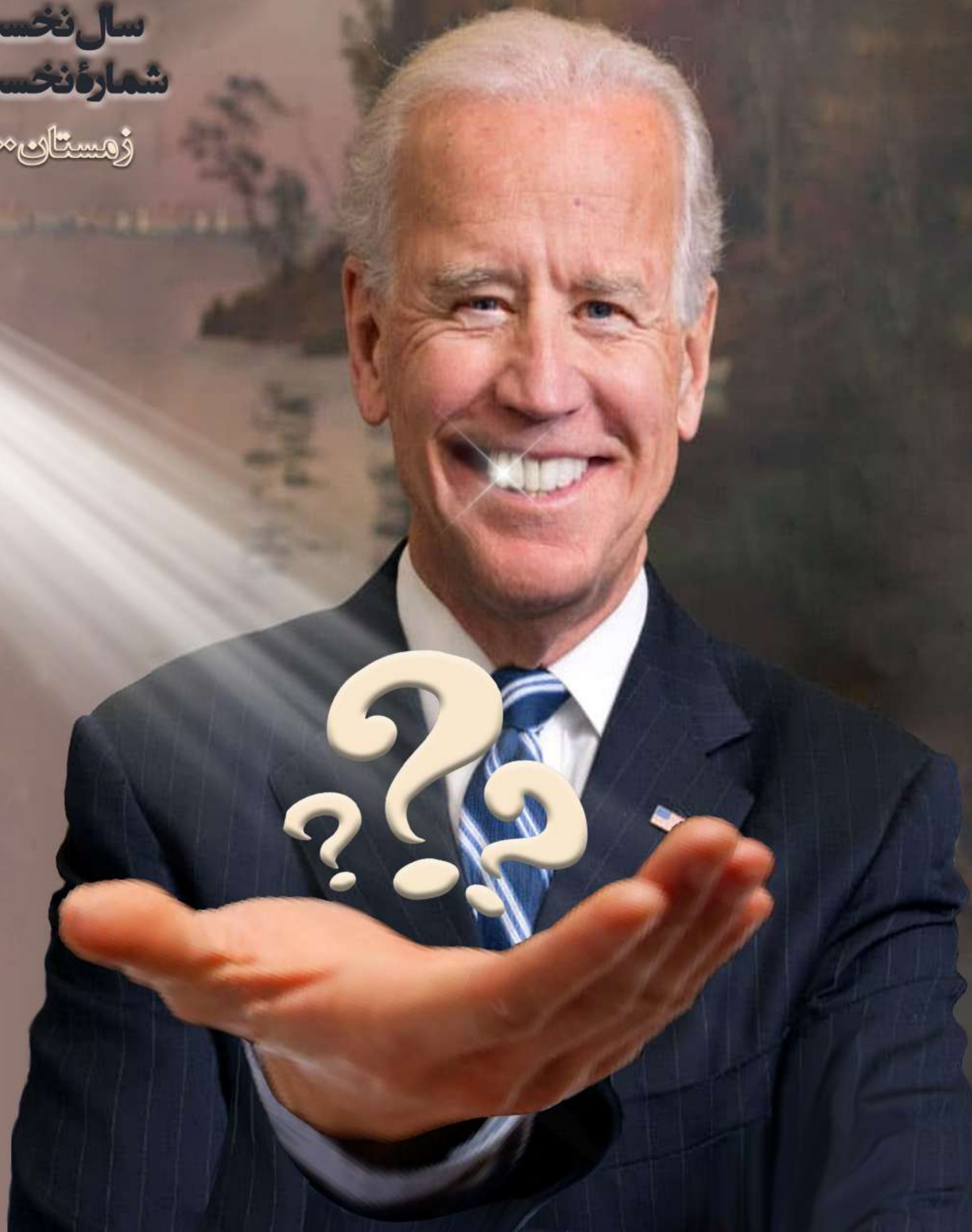
فصلنامه

نوای شرق

سال نخست
شمارهٔ نخست
زمستان ۱۴۰۰



ارگان پایگاه تحلیلی سهیل رسانه
سردبیر: حیدر سهیلی اصفهانی
https://sohailmedia.ir
سهیل رسانه

زمستان ۱۴۰۰

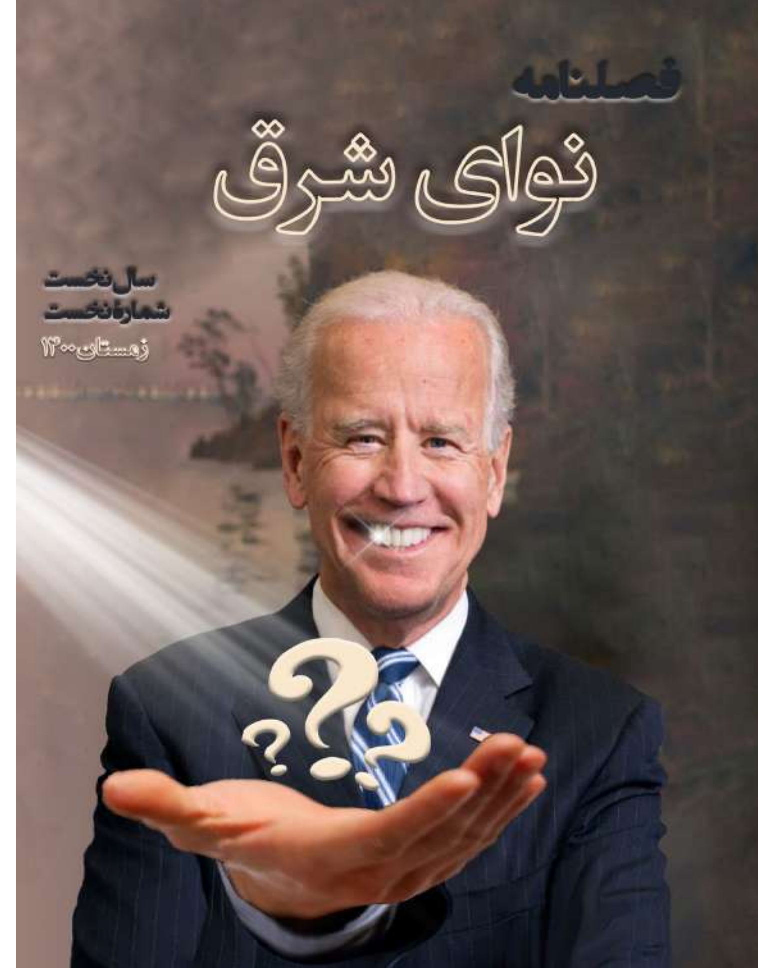
نوای شرق

نگاهی تحلیلی به جهان پیرامون

نخستین بار، نشریه‌سازیم را با نوای شرق شروع کردم. ماهنامه‌ای بود که نوشته‌های مرا با نوشته‌های قدیم و جدید دیگران در هم می‌آمیخت و دست آخر، چیزکی درست می‌شد که من نشریه نساخته از دنیا نروم. ارزش آن را داشت که من با شیوه‌های فنی چاپ و نشر دیجیتال آشنا شوم. خراب کنم و بعد درست کنم و یاد بگیرم. وقتی که یاد گرفتم، بی‌تعارف آن را کنار گذاشتم و مدتی آن را به بازنشستگی فرستادم.

چرا؟ چون وقتی ندانی چه باید بنویسی، همان موقع باید قلم را کنار بگذاری..!

کل ژورنالیسم و مکاتب مختلف نویسندگی، اعم از نثر و نظم، یک آفت بزرگ و مشترک دارند؛ بی‌هوده نویسی! هیچ کس از ننوشتن نمی‌میرد... پس زنده‌باد



آن کس که اوقات فراغت خود را به دیدن فیلم‌های خوب، یا حتی دیدن مسابقهٔ فوتبال بگذراند، اما بی‌هوده ننویسد!

به علاوه، ماهنامهٔ نوای شرق، هووی بزرگی هم یافت و آن نشریهٔ فکاهی بود که نامش را گذاشتم؛ مجلهٔ فکاهی ملانصرالدین... سبکی در تحلیل سیاسی که قوامش طنز است و آن را از مولانا عبید زاکانی، بزرگ مرد تحلیل سیاسی آموختم. چون پس از سال‌ها خواندن نظریات دانشمندان داخلی و خارجی، در نهایت، از او یاد گرفتم که واقعیت خنده‌دار است. شمارگانش که به ۳۷ رسید، باز هوای نشریه‌ای برای تحلیل جدی، مرا در سر افتاد و باز یار دیرین به بازنشستگی فراخوانده را فراخواندم.

آیا چیز تازه‌ای برای نوشتن یافته بودم؟ بعله..!

تصمیم گرفتم مقالات پر بار غربی را که به زبان‌های بیگانه منتشر می‌شود، ترجمه کنم. ماجرای همان کس شد که دید دو بزرگ را به زندان می‌برند، خود را در میان انداخت و گفت: «ما سه تا را دارین کجا می‌برین؟»

حالا من و نویسندگان مبرز فارین افیرز و فارین پالیسی، نیوزویک و تایم، گاردین و ایندیپندنت و دیگران، با هم فصلنامه‌ای به نام «نوای شرق» منتشر کرده‌ایم. به هر حال، به آن‌ها افتخار دادم که مرا همراهی کنند.

چرا فصلنامه است؟ چون راستش آن قدرها وقت ندارد که خود را درگیر ماهنامهٔ دیگری کنم. تازه قرار است همهٔ کارهایش را خودم تنهایی و یک نفره بکنم. هیچ وقت به خودم دغدغه ندادم که آیا نوشته‌های مرا کسی می‌خواند یا نه... یاد مادر مرحومم به خیر که غذا می‌پخت و می‌گفت: «شام آماده است. هر کی می‌خواد، بیاد بخوره! هر کی هم نمی‌خواد، بره گشنه بخوابه!»

من و ما می‌نویسیم. آن کس که گرسنهٔ دانستن است، بفرماید و بخواند و هر کس، نه! نمی‌خواهد مغزش از تنظیمات کارخانهٔ الهی خارج شود، بر همان تنظیمات بماند.

من و ما می‌نویسیم و چون روزی را حضرت حق بی‌منت فرستاده، ما هم بی‌منت، به رایگان هبه می‌کنیم. هر کس خواست بخواند و هر کس نخواست، بر او حرجی نیست. به قول استاد سخن؛

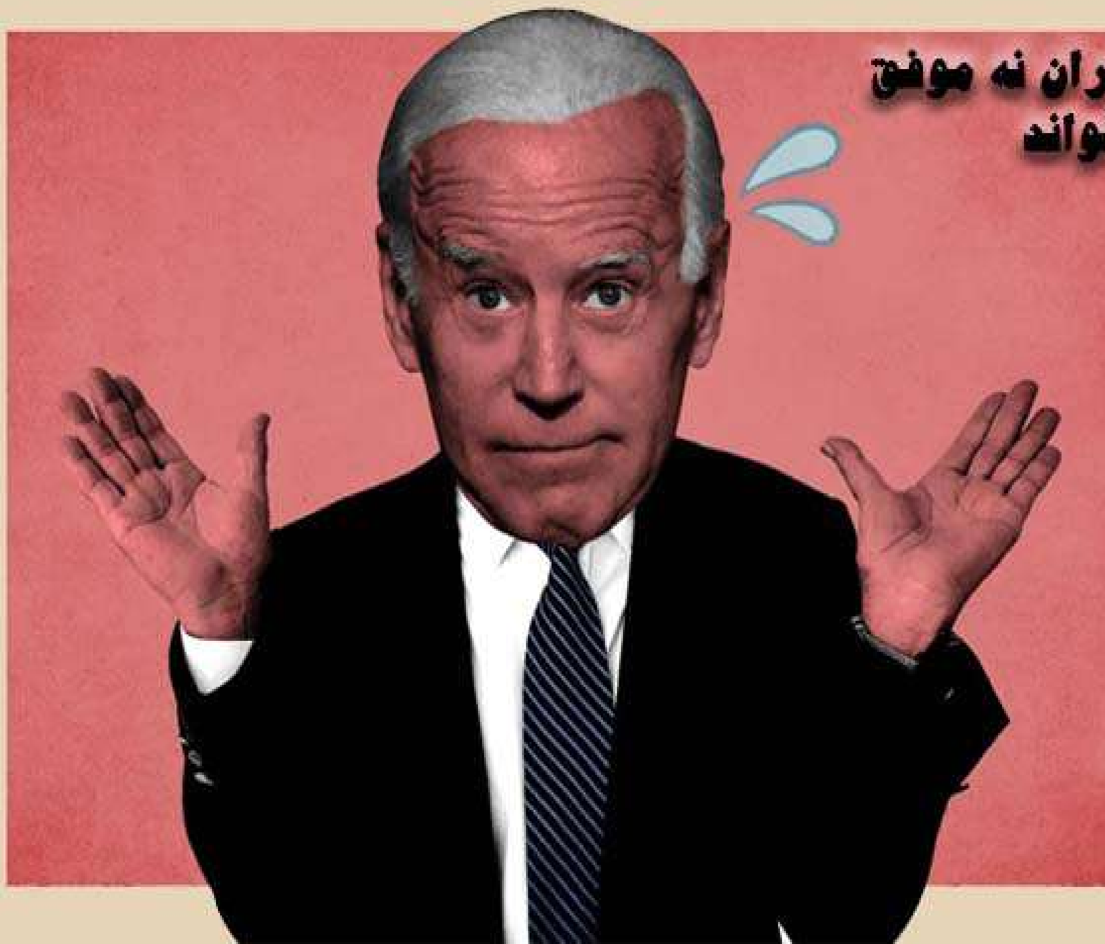
تو نیکی می‌کن و در دجله انداز
که ایزد در بیابانت دهد باز

حیدر سهیلی اصفهانی

مذاکرات هسته‌ای ایران نه موفق خواهد شد و نه می‌تواند موفقیت آمیز باشد!

دیوید فارس









کافی است تا مذاکرات تقریباً قطعا محکوم به فنا بین رهبران ایران و اروپا در وین را در این ماه مشاهده کرده باشید تا متوجه شوید که تلاش‌های جاری به منظور استفاده از دیپلماسی برای محدود کردن برنامه تسلیحات هسته ای تهران به مراحل پایان‌اش نزدیک شده است. وقتی این گفتگوها به ناگزیر متوقف شوند، دهه‌ها توهم را به خاک می‌سپارند و بنای درهم ریخته سیاست خارجی آمریکا را آشکار می‌سازند. چوب‌های پوسیدهٔ آبروی آمریکا از پس تزئینات بیرون خواهد زد و چند دستگی‌های داخلی هر روز زشت تر از دیروزمان، دیگر پشت زورق دیپلماسی پنهان نخواهد ماند.

مذاکرات از زمان نگارش این مقاله متوقف شده است، اما قرار است هفته آینده از سر گرفته شود. گو آن که دیپلمات های اروپایی در حال حاضر بسیار بدبین به نظر می‌رسند. آنتونی بلینکن، وزیر امور خارجه، روز جمعه گفت: رهبران ایالات متحده به سوی تهدیدات تلویحی به کاربرد زور باز خواهند گشت؛ «ما یا به توافق برمی‌گردیم، یا باید حل و فصل این مشکل را از راه های دیگر بررسی کنیم.». در حالی که ایران در حال افزایش تقاضاهای خود است . تهران خواستار آن است که درصد غنی‌سازی‌اش را افزایش دهد و همچنین تضمینی می‌خواهد تا در صورت پیروزی جمهوری‌خواهان در دورهٔ بعد انتخابات ریاست جمهوری، ایالات متحده دوباره این توافق را از ریشه درو نکند.

نیازی نیست در آزمون روابط خارجی شرکت کرده باشید تا متوجه شوید که چرا این مشکل هر بار پیچیده‌تر می‌شود: ایران رئیس جمهور جدید و تندرویی، به نام ابراهیم رئیسی دارد که باور نمی‌کند ایالات متحده تا پایان به تعهدات خود پایبند می‌ماند. دلیل موجهی هم دارد؛ در سال ۲۰۱۸، دولت ترامپ بی هیچ دلیلی، جز گستاخی و کینه توزی از برنامه جامع اقدام مشترک (برجام) ۲۰۱۵ که به توافق هسته ای ایران معروف است، خارج شد. آن توافق، فعالیت‌های غنی‌سازی ایران را محدود کرده بود و در ازای لغو تحریم‌ها، این کشور را تحت بازرسی‌های سرزدهٔ آژانس بین‌المللی انرژی اتمی (IAEA) قرار داده بود. در حالی که بیشتر جمهوری خواهان به چارچوب توافق اعتراض داشتند، اما هیچ کس، هیچ مدرک معتبری دربارهٔ تقلب ایران ارائه نکرده است.

نمایش تحقیرآمیز دونالد ترامپ، اقتصاد ایران را به رکود کشاند و سختی‌های بی‌شماری را بر مردم ایران تحمیل کرد، در حالی که مطلقاً هیچ دستاوردی نداشت. پس از این که ایالات متحده، برجام را نابود کرد، ایران تلاش‌هایش را برای افزایش توانمندی‌هایش در حوزهٔ غنی سازی افزایش داد و امکانات بازرسان برای نظارت بر فعالیت های هسته ای خود را محدود کرد. امروزه، ایران احتمالا در حال غنی‌سازی اورانیوم است (فرآیند پیچیده‌ای برای افزایش غلظت ایزوتوپ U-۲۳۵ به ۲۰ درصد تا سوخت نیروگاه‌های هسته‌ای را تامین کند). اگر این غلظت به ۹۰ درصد برسد، می‌توان بمب‌سازی را شروع کرد. هرچند تهران همیشه قصد انجام این کار را رد کرده است.

شایان ذکر است که در وهله اول، هدف توافق، کلا جلوگیری از رسیدن ایران به چنین مرحله‌ای بود و توافقی که ترامپ آن را به شکست کشید، نشان دهنده نقطهٔ اوج بیش از یک دهه دیپلماسی اغلب کینه توزانه، همراه با آغازی دروغین بود. دولت ترامپ، با منطقی آن قدر متزلزل که نمی‌توان آن را جدی گرفت، ادعا کرد که توافق با ایران احتمال دستیابی ایران را به سلاح‌های هسته‌ای افزایش می‌دهد و مدعی بود که این برون رفت، تهران را وادار می‌کند که به میز مذاکره بازگردد. یعنی یا مذاکره کنندگان جمهوری اسلامی به راحتی در برابر شرایط آمریکا سر تسلیم فرود می‌آورند و یا با حملات هوایی توفنده رو به رو خواهند شد.

نیازی به گفتن نیست که ایران با دولت ترامپ مذاکره نکرد و هیچ حمله هدفمندی هم از سوی ایالات متحده انجام نشد، اما پیامد بلندمدت مهمتر این است که ترامپ ممکن است برای همیشه اعتبار آمریکا را خدشه دار کرده باشد. چرا طرف‌های مذاکره کننده باید بپذیرند که تصمیمات و توافقات سیاست خارجی ایالات متحده می تواند از تغییر قدرت اجرایی در واشنگتن جان سالم به در ببرند؟ دولت های دیگر نیم دوجین سال را صرف مذاکره برای توافقی نمی کنند که فقط دو یا سه سال دوام بیاورد. وضعیتی که ترامپ ایجاد کرده است، چیزی شبیه معمای زندانی است، آزمایشی فکری که محققان روابط بین‌الملل برای درک مشکلات ذاتی دولت‌ها

در اعتماد به یکدیگر در قلمرو هرج‌ومرج سیاست جهانی، از آن بهره می‌گیرند. تصور کنید شما و یکی از دوستانتان تصمیم به انجام جنایت سبکی می‌کنید و از قبل موافقت می‌کنید که اگر گرفتار شدید، چیزی نگویید. متأسفانه، معلوم می‌شود که شما کلاهبردار هستید و دستگیر می‌شوید و پس از آن، کارآگاهان بلافاصله شما را به اتاق‌های بازجویی جداگانه‌ای می‌فرستند.

اگر هر دو چیزی نگویید، احتمالاً یک سال زندان کوتاه مدت خواهید داشت. اما اگر دوستت را مقصر بدانی و او ساکت بماند، سه سال به او می‌رسد و تو آزاد می‌شوی و برعکس. اگر هر دوی شما یکدیگر را بفروشید، محکومیتتان دو سال خواهد بود. بدتر از این که به معامله پایبند باشید، اما بهتر از این که لو داده شوید. اگر به همدیگر اعتماد نکنید، هر دو در نهایت وضعیت بدتری خواهید داشت.

بسیاری از محققان روابط بین الملل معتقدند که این منطق اساسی در مورد انواع تعاملات بین کشورها، از جمله مذاکرات تغییرات آب و هوا، توافقنامه‌های کنترل تسلیحات و محدودیت های ماهیگیری اعمال می‌شود. دولت‌ها بهتر است از شرایط موجود، مثلاً توافقی برای کاهش ذخایر سلاح‌های هسته‌ای یا حفاظت از جمعیت ماهی تن پیروی کنند. در ازای کمی ناراحتی، هر دو طرف از یک نتیجه بدتر جلوگیری می‌کنند. اما همان طور که هیچ کس، اجرای توافق بین دو جنایتکار کوچک را تضمین نمی‌کند، هیچ حاکم جهانی نیز وجود ندارد که متقلبانی را مجازات کند که مخفیانه هزاران سلاح اتمی می‌سازند یا اقیانوس هر ماهی را غارت می‌کنند.

گوش کسی به این حرف‌ها بدهکار نیست، اما نظریه‌پردازان باهوش بازی‌ها که این افسانه کوچک را ساخته‌اند، فکر می‌کنند راهی برای تغییر محاسبات فاجعه‌بار به سبک کوبایاشی Kobayashi Maru مارو وجود دارد که نوعی تمرین، به‌طور نامحدودی تکراری است. به عبارت دیگر، اگر انتظار دارید دوباره با دوست خود همکاری کنید، به احتمال زیاد به قول هایی که به یکدیگر داده‌اید، پایبند خواهید بود. ایجاد روابط پایدار و فرصت‌های معمول برای همکاری و حل مناقشه بین دولت‌ها، روشی است که ناظران بر این باورند نهادهای بین‌المللی، با



وجود این که کلانتری در شهر وجود ندارد، درگیری را کاهش می‌دهند.

توافق با ایران می‌توانست شروعی برای تقویت اعتماد بین واشنگتن و تهران باشد. درعوض، ترامپ در این بازی، ایران را فروخت.

و این اولین بار هم نبود؛ در آغاز دههٔ ۱۹۹۰، ایالات متحده از معاهده‌های متعددی، یکی پس از دیگری بیرون رفت. گاهی اوقات، از توافق نامه های موجود (مانند معاهده موشک های ضد بالستیک) خارج شد و گاهی سنای ایالات متحده، معاهدات رسمی را تصویب نکرد(مانند معاهده منع مین در سال ۱۹۹۷) یا اخیراً، خواستار بازنگری یک طرفه در یک توافق موجود شد (مانند اصرار دولت ترامپ بر مذاکره مجدد دربارهٔ توافقنامهٔ تجارت آزاد آمریکای شمالی). در مجموع، این جنجال‌ها، اعتماد دیگر کشورها را به دیپلماسی آمریکایی سخت‌تر کرده است، به‌ویژه زمانی که حزب جمهوری‌خواه در راس قدرت است. سابقهٔ طولانی دشمنی و درگیری بین ایالات متحده و ایران، غلبه بر خیانت‌های گذشته را حتی سخت‌تر می‌کند، به ویژه زمانی که همان حزب جمهوری خواه آشکارا در حال طراحی کودتا برای سال ۲۰۲۴ است. تهران می‌داند که خاورمیانه آخرین جایی است که دولت بایدن می‌خواهد سرمایهٔ سیاسی محدود خود را خرج کند و پس از نزدیک به بیست سال تهدید به حمله که هرگز محقق نمی شود، مذاکره کنندگان ایران را می توان بخشید که چنین تهدیدهایی را نمایش می پندارند.

در نهایت، ایران تضمین هایی را که می‌خواهد در این جا دریافت نخواهد کرد. واشنگتن مستقیماً در این گفتگوها شرکت نمی‌کند و رئیس جمهور بایدن نمی‌تواند مطمئن باشد که جانشینش چه خواهد کرد. بنابراین، در غیاب مقداری نبوغ در وین، این بحران احتمالاً به شکل کنونی‌اش ادامه خواهد یافت و همهٔ طرف‌ها وضعیت بدتری خواهند داشت، تا زمانی که ایران بالاخره، سلاح هسته‌ای بسازد یا رئیس‌جمهور بعدی ایالات متحده، یک بار دیگر، نبرد بی‌رحمانه و چند دهه‌ای و بی‌نتیجه‌ای را راه اندازی کند که هدفی جز ایران ندارد.

در آن مرحله، کاملاً مشخص خواهد شد که بازنده در تمام مدت چه کسی بوده است.

رابرت فیسک، زاده ۱۲ ژوئیهٔ ۱۹۴۴ در میدستون – درگذشته ۳۰ اکتبر ۲۰۲۰ در دوبلین، نویسنده و روزنامه‌نگار انگلیسی-ایرلندی بود.
وی خبرنگار بین‌المللی بود و جنگ‌های داخلی لبنان، الجزایر و سوریه، جنگ ایران و عراق، جنگ‌های بوسنی و کوزوو، جنگ شوروی در افغانستان، انقلاب ۱۳۵۷، حمله صدام حسین به کویت ،جنگ خلیج فارس و اشغال عراق را پوشش داد. او در اواخر عمر، مسئولیت بخش خاورمیانه‌ای روزنامهٔ انگلیسی ایندیپندنت را برعهده گرفت. مقالات او در این روزنامه، شاهکار تحلیل خبر به شمار می‌رود.



رابرت فیسک، برند متفاوتی در تحلیل

حیدر سهیلی اصفهانی

در جریان رویدادهای درۀ پنج شیر، در به در در پی آخرین تحلیل رابرت فیسک می‌گشتم؛ اما تنها با یک خبر رو به رو شدم و آن هم خبر درگذشت این اعجوبۀ تحلیل، ماه‌ها پیش بود. کسی که در طول دوران فعالیتم در گروه تحقیق و تفسیر خبر، خرقۀ شاگردیش را آگاهانه بر دوش انداخته بودم و بدون آن که اصلا مرا بشناسد، به شاگرد مع الواسطه‌اش تبدیل شده بودم

رابرت فیسک، تحلیلگر و رئیس بخش خاورمیانه‌ای روزنامۀ انگلیسی ایندیپندنت بود. هر کس اهل خواندن مقالات سیاسی باشد، خیلی راحت می‌تواند قدرت مقالات نویسندگان انگلیسی مثل رابرت فیسک





یا پاتریک کوکبرن را بر هم‌آوردان آمریکایی مثل دیوید اگناسیوس یا راجر کوهن یا حتی برندهایی مثل شیرین هانتر درک کند؛ اما قطعا رابرت فیسک کس دیگری در این میان بود که عملکردش و روش‌های تحلیلش و متدولوژی‌اش با همه فرق داشت، حتی با همکاران انگلیسیش.

- جوگیر نبود

برای تحلیلگران آسان‌ترین راه آن است که روی موج خبرهای جاری سوار شوند و خیلی توفنده به همان نتایجی برسند که جو حاکم آن را به مردم خورانده است. اما در عین حال، بدترین اتفاق در تحلیل همان است که تحلیلگر، در پی چنین موجی بدود. امروز مطابق موج و فردا شاید وقتی مسیر موج تغییر کند، مخالف همین موج بنویسد.

قطعا رابرت فیسک این طور نبود. در هنگامه‌های تحلیل که در روزنامه‌های آمریکایی و حتی بعضا انگلیسی، خط فکری مشابهی حاکم بود و در مقالات آمریکایی منتشره در نشریات مهمی در حد نیویورک‌تایمز، خزعبلاتی خنده‌دار منتشر می‌شد، از رابرت فیسک چیزی جز سکوت نمی‌دیدید.

رابرت کجاست؟ واقعا چرا ساکت است؟ همه در حال چه چه زدن و او در سکوت مطلق..! چند هفته بعد، متوجه اشتباهمان می‌شدیم. خبر در سوریه است؟ او در این چند هفته در سوریه بود. با یک دوربین در دست و کیف کوچکی بر دوش..! در این مدت حتی با بشار اسد و رهبر مخالفانش صحبت کرده بود و نیز با مردم عادی در کوی و برزن! آن گاه مقاله‌ای پر از اطلاعات ناب دست اول منتشر می‌کرد. دربارۀ چه؟ دربارۀ ارتش سوریه!

او در آن مقاله خطاب به غرب می‌گفت: "این موج را برای نابودی ارتش سوریه بر پا کرده‌اید، اما اتفاقا به همین سبب، ارتش سوریه در حال تبدیل به ارتشی بسیار متفاوت و تهدید بزرگی برای اسرائیل شده است." هر کس تحلیل رابرت فیسک را می‌خواند، امروزه می‌توانست بفهمد چرا اسرائیل به بهانۀ حمله به نیروهای ایرانی، در حال زدن پادگان‌های ارتش سوریه است، آن هم خیلی دیر! شاید به این سبب که در زمان انتشار آن مقاله، مقام‌های اسرائیلی به جای خواندن آن، در حال رقص پوریم بودند.

- متدولوژی او

چیزی که در او توجهم را جلب کرد، متدولوژی بسیار نیرومندش در درک مسائل روز بود. از دید او، تحلیلگر باید در پی اطلاعات دست اولی باشد که همه به آن بی‌توجهی می‌کنند. چرا این وضع پیش آمده است؟ باید با دقت، اطلاعات مربوطه را گرد آورد و به نتیجه رسید.

در یکی از مقالاتش که طبق معمول، پس از سفر به یمنِ آرام، گرچه کمی متشنج به سبب تظاهرات نوشت، برخلاف تصور همه، او به دنبال ریشه‌های بحران یمن نرفت و سخنان صد من یک غازی را که همه بلدند، تحویل خواننده نداد.

از یمن بازگشت تا خبر بدهد: جنگ داخلی بزرگی در یمن در راه است. چرا؟ چون ۴۴ میلیون قبضه سلاح سبک در یمن انباشته شده است. هیچ کس نمی‌فهمید او چه می‌گوید. او در مقام استاد، به همه درس داد که هر کجا سلاح سبک انباشت شد، جنگ داخلی بزرگی در راه است. نه سلاح سنگین!

مدتی بعد، در حد چند ماه، آتش جنگ یمن برپا شد و بیش از همه، این رابرت فیسک بود که فهمید: این جنگ مهندسی شده است. برای این جنگ زمینه‌چینی شده است. آن هم کی؟ زمانی که همه فقط به تظاهرات محدود در صنعا و عدن نگاه می‌کردند.

او به منِ تحلیلگر آموخت، برای آشنایی با هر جا، اول از همه از موج خبر دوری کن... چون سیلابی است که تو را می‌برد. دوم، به اطلاعات زیربناییِ اتفاقی که در راه است، دست پیدا کن.

-منع هواداری در تحلیل

درس سوم او صداقت با خود بود. رابرت به من، این شاگردی که هیچ گاه ندید و با او آشنا نشد، آموخت: هیچ وقت خود را فریب نده. هیچ وقت در استخدام پروژه‌ای قرار نگیر و در این راه، آن چنان بی‌طرف باش که مطالب تو را طیفی از تناقضات شکل دهد. هیچ کس از مطالبت نتواند بفهمد که تو طرفدار چه طیفی هستی؟ چون یک تحلیلگر حق ندارد طرفدار باشد. شغل و کسوت تحلیلگری، آن قدر شرافت دارد که تحلیلگر هوادار شغل خودش باشد.

اکنون که میرزا بنویس‌ها در استخدام خودخواستۀ این یا آن طیف سیاسی قرار می‌گیرند و از این جماعت میرزا بنویس، در ایران، آمریکا، اسرائیل، خصوصا کشورهای عرب و کلا همه جا به فور یافت می‌شود، با خواندن مطالب رابرت فیسک، انسان می‌تواند درک کند که تحلیل اصولا چگونه شغلی است و چرا اغلب مفسران، قطعا تحلیلگر نیستند.

- درگذشت

این اعجوبۀ تحلیل که در سال ژوئیۀ ۱۹۴۴ چشم به جهان گشوده بود، سرانجام، در سی‌ام اکتبر ۲۰۲۰، بر اثر سکتۀ قلبی چشم بر جهان بست، بی‌آن که جانشین شایسته‌ای برای مکتب تحلیلی‌اش بر جای بگذارد. اکنون صدای تحلیل صادقانه و بی‌طرفانه، در میان هیاهوی مفسرانی که واقعیت را بر اساس صلۀ دریافتی بیش و کم می‌کنند، بسیار بی‌رمق است. شاید این جا و آن جا در این کرۀ خاکی، چند تایی پیدا شوند. کم صدا، کم اثر، بی‌رمق..!

یادش گرامی!

چگونه به خطر اومیکرون برای کودکان فکر کنیم؟

آنا واتس برای نیویورک تایمز



سویهٔ اومیکرون در گسترهٔ وسیعی در حال گسترش است و خطر ابتلا به عفونت بیشتر از قبل است. این امر برای والدین، به ویژه آن‌هایی که کودکان بسیار کوچکی برای واکسینه شدن دارند، بی‌اعتمادی ایجاد کرده است. ما از دو متخصص دربارهٔ چگونه فکر کردن در این زمینه پرسیدیم. ما این پاسخ‌ها را ویرایش کردیم تا هم کوتاه‌تر شوند و هم واضح‌تر.



• جنیفر نوزو Nuzzo ، اپیدمیولوژیست در دانشکده بهداشت عمومی جانز هاپکینز بلومبرگ که حوزهٔ تخصصی‌اش بیماری‌های عفونی است. دکتر نوزو همچنین مادر دو فرزند ۵ و ۸ ساله است که در مدرسه دولتی تحصیل می‌کنند و کاملاً واکسینه شده‌اند.

– بچه های من خیلی کوچک‌تر از آن هستند که واکسینه شوند. پس باید در بارهٔ خطر اومیکرون نگران باشم ؟

جنیفر نوزو: من والدین زیادی را در این شرایط می شناسم که بسیار نگران هستند. من واقعا با آن‌ها احساس هم دردی می‌کنم. پدر و مادر کودکان خردسال بودن، به اندازه کافی دردسر دارد، چه برسد به آن که بیماری فراگیری نیز شایع شده باشد.

من به طور کلی سعی می کنم مردم را تشویق کنم که به این خطر به دو شکل فکر کنند: خطر ابتلا و خطر ابتلای جدی به بیماری. سطح ابتلای وسیع در جامعه، خطر ابتلا را در تمام سنین افزایش می‌دهد. با این احتمال که اومیکرون باعث افزایش موارد ابتلای کووید در جوامع شود، با کمال تاسف، احتمال ابتلا نیز به همان اندازه افزایش خواهد یافت.

اما واکسیناسیون کودکان تنها راه محافظت از آن‌ها نیست. به طور کلی، ما دیده‌ایم که می‌توانیم با اطمینان از این که بزرگسالان پیرامون کودکان واکسینه شده‌اند، محافظت از کودکانِ واکسینه نشده را افزایش دهیم. این امر، روش مهمی برای محافظت از کودکانی است که برای واکسینه شدن بسیار کوچک هستند.

همچنین می توانید با پرهیز از حضور در فضاهای شلوغ، سرپوشیده و سایر اجتماعات، استفاده از تست های سریع قبل از رویدادهای اجتماعی و استفاده بزرگسالان از ماسک در برابر کودکان خردسالشان، خطر قرار گرفتن فرزندتان در معرض ویروس را کاهش دهید.

دربارهٔ خطر ابتلا به بیماری در کودکان خردسال، خوشبختانه، همه داده‌هایی که ما در اختیار داریم نشان می‌دهد که خطر ابتلا به بیماری شدید در صورت آلوده شدن آن‌ها بسیار کمتر از بزرگسالان و نوجوانان است. داده های جدید همچنین نشان می‌دهد که خطر ابتلا به کووید طولانی در میان کودکان نیز کم است. اگر نوزادان زیر 12 ماه داشته باشیم، اقدامات احتیاطی بیشتری انجام می‌دهیم، زیرا ممکن است خطر بیماری شدیدتری در مقایسه با کودکان نوپا داشته باشند. اما خوشبختانه، محدود کردن قرار گرفتن در معرض نوزادان آسان‌تر است، زیرا بسیاری از آن‌ها در آن سن، تحرک چندانی ندارند. کودکان مبتلا به بیماری‌های زمینهای ای بسا در معرض خطر بیشتری باشند و والدین باید برای دریافت راهنمایی‌های خاص، با پزشک کودکشان مشورت کنند.

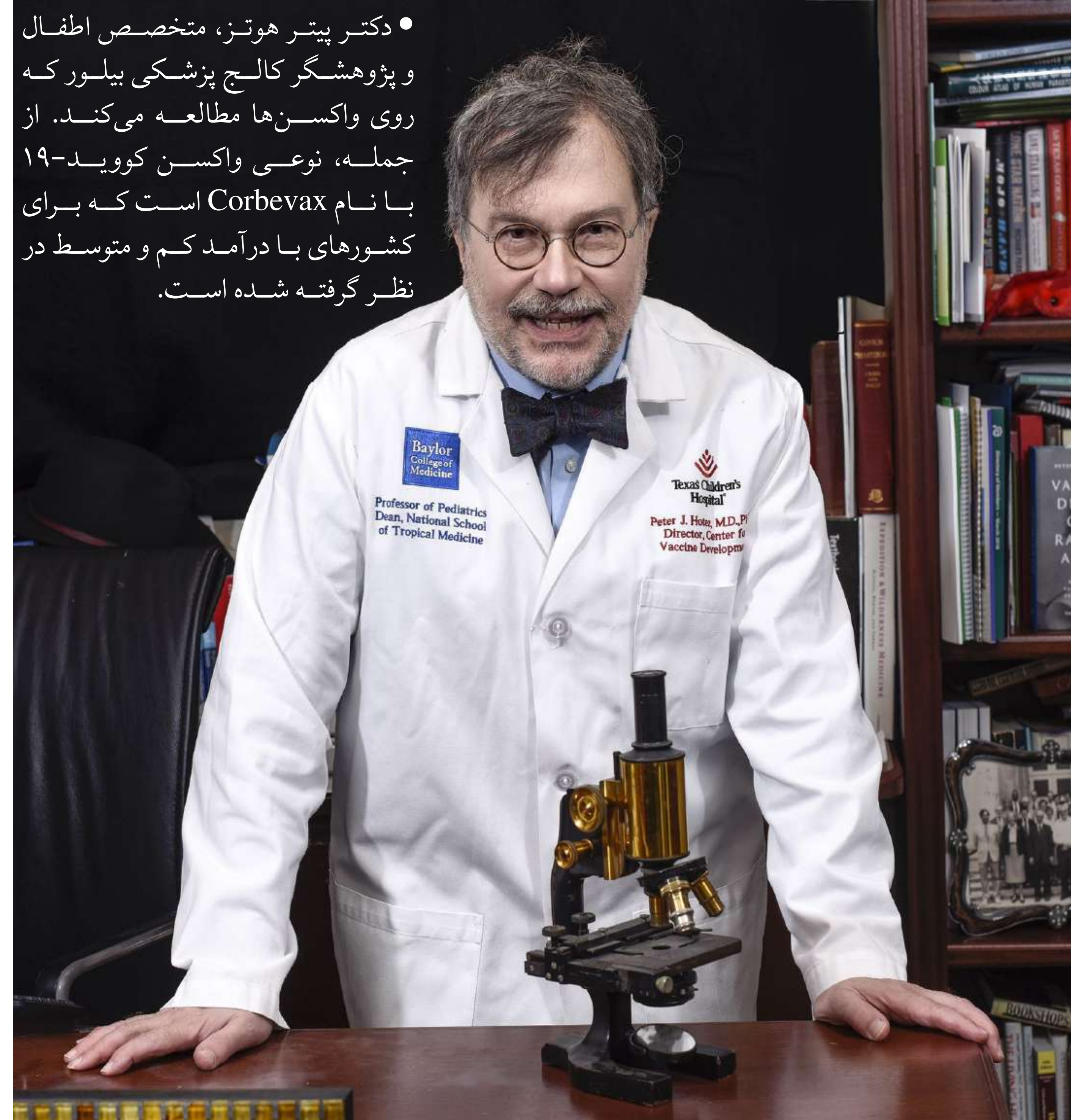
در حالی که هنوز زود است، ما هنوز هیچ داده‌ای دربارهٔ سویهٔ اومیکرون ندیده‌ایم که ما را نگران کند که خطر ابتلا به بیماری شدید در بین کودکان تغییر کرده است. این خطرات نسبتاً کم و توانایی ما برای کاهش بیشتر آن‌ها ممکن است به کاهش برخی از اضطراب‌ها در چند ماه آینده کمک کند.

پیتر هوتز: موافقم! همچنین اضافه می‌کنم که در آفریقای جنوبی، شاهد بوده‌ایم که کودکان خردسال مبتلا به سویهٔ اومیکرون گاهی به بستری شدن در بیمارستان نیاز پیدا کرده‌اند. با این حال، تعدادی از این کودکان ممکن است با ابتلا به کووید در بیمارستان بستری شده باشند، اما نه به دلیل ابتلا به کووید. بعید است که اومیکرون منحصرا کودکان را هدف قرار داده باشد، اما از آن جایی که این سویه قابلیت انتقال بسیار سریعی دارد، می‌تواند موجی توفنده را بر پا کند و کودکان را هم همراه با بزرگسالان در این موج غرق کند. شبیه به همان وضعی که در تابستان گذشته، سویهٔ دلتا برای کودکان در همین جا تگزاس به راه انداخت.

– مدرسه فرزندم یک کلاس را به دلیل موارد جدید ابتلا به کرونا تعطیل کرده است. حالا با نمره‌های بچه‌هایمان چه کار کنیم؟

جنیفر نوزو: کارشناسان بهداشت عمومی ترجیح می‌دهند در بارهٔ ایمنی به صورت نسبی صحبت کنند؛ "ایمن تر" به "ایمن". به طور کلی، مدارسی که از استراتژی‌های کاهش موارد ابتلا استفاده می‌کنند، احتمالا در مقایسه با دیگر محیط‌های اجتماعی، محیط امن‌تری برای کودکان هستند.

خطرات جدی بیماری در کودکان، در طول دورانِ همه گیری کم بوده است و دانش آموزان در سن مدرسه



• دکتر پیتر هوتز، متخصص اطفال و پژوهشگر کالج پزشکی بیلور که روی واکسن‌ها مطالعه می‌کند. از جمله، نوعی واکسن کووید-۱۹ با نام Corbevax است که برای کشورهای با درآمد کم و متوسط در نظر گرفته شده است.

اکنون می‌توانند برای کاهش بیشتر خطر ابتلا به بیماری‌های جدی واکسینه شوند. جزئیات مهم هستند. برای مثال، از تلاش‌هایی که برای ردیابی تماس‌های مدرسه دربارهٔ منبع احتمالی ابتلای همگانی صورت می‌گیرد، چگونه می‌توان نتیجه گرفت؟ در بسیاری از موارد، وجود ابتلا در کلاس درس، ای بسا ناشی از شیوع بیماری در داخل مدرسه نباشد، بلکه ریشه در فعالیتی اجتماعی یا فوق برنامه باشد که همکلاسی‌ها در آن شرکت کرده‌اند.

به طور کلی، موارد ابتلا در میان باشندگان محیط مدرسه بسیار نادر است. اگر مدارس، روش «آزمایش برای ماندن» را اجرا کنند، می‌توان این خطر را کاهش داد. یعنی به‌جای الزام اجبار افرادِ مرتبط با مبتلایان به قرنطینه،

از آزمایش‌های سریع در طول دوره قرنطینه استفاده شود تا مشخص شود آیا این افراد مرتبط، برای حضور در مدرسه ایمن هستند یا خیر. مرکز کنترل و پیشگیری از بیماری اخیراً این سیاست را تأیید کرده است.

هوتز: در این موج ابتلا به اومیکرون، حاشیهٔ امن زیادی وجود ندارد، اما حداقل اکنون در زمانی که کودکان برای تعطیلات زمستانی یا کلا تعطیلات هفتگی به خانه فرستاده می‌شوند، شتاب بیشتری می‌گیرد. بنابراین، مهد کودک‌ها، مدارس، بیشتر

کالج‌ها و دانشگاه‌ها، در زمانی که موارد ابتلا در بدترین حالت خود هستند، تشکیل جلسه نخواهند داد. در ماه ژانویه، ممکن است بازگشایی‌های با تأخیر روی دهد، به‌ویژه اگر در حال حاضر در شیب این موج جدید قرار داشته باشیم و یک یا دو هفته بیشتر منتظر بمانیم، اما مانند هر سویهٔ جدیدی، ما تا زمانی که واقعا ندانیم، نخواهیم دانست.

– آیا در فضای باز، اومیکرون در مقایسه با دلتا خطر بیشتری دارد؟ آیا کودکان باید در زمین‌های بازی ماسک بزنند؟

جنیفر نوزو: من اطلاعات خاصی ندیده ام که اومیکرون، خطر انتقال در فضای باز را افزایش دهد. همگام با هر کدام از اقدامات ایمنی که در پیش می‌گیریم، ما باید میزان حفاظتی را که این اقدام اضافه می‌کند، در مقابل درجه اختلالی که ایجاد می‌کند، متعادل کنیم. مهم ترین مکان ماسک در داخل خانه است. برخی از بچه ها از بستن ماسک در زمین‌های بازی کاملاً خوششان می‌آید، به خصوص اگر هوا خیلی گرم نباشد. اما سایر کودکان، واقعاً از کندن ماسک استقبال می‌کنند.

– مدرسه فرزندانم، آن‌ها را مجبور نمی‌کند در طول تعطیلات در فضای باز ماسک بزنند و فرزندانم هم از این بابت، بسیار خوش حالند که بعد از بستن ماسک در مدرسه، در طول روز، حالا کمی استراحت کنند. من از این حمایت می‌کنم. خانواده‌ام معمولاً وقتی در خارج از منزل هستیم، ماسک نمی زنند، اما اگر در جمع باشیم، همگی ماسک می‌زنیم.

جنیفر نوزو: پاسخ به این سوال به موقعیت خاص فرزندان شما و سطح تحمل خطر شما بستگی دارد. فرزندان من هر دو واکسینه شده‌اند، بنابراین من با خیالی راحت، آن‌ها را به موزه می‌برم. اگر آن‌ها بیماری زمینه‌ای داشتند، به طوری که من نگران سطح محافظت آن‌ها، در برابر واکسن یا خطر ابتلا به بیماری شدید در صورت ابتلایشان بودم، احتمالاً سعی می‌کردم تا حد زیادی از فضاهای داخلی شلوغ اجتناب کنم.

قبل از این که فرزندانم بتوانند واکسینه شوند، ما در مورد جایی که آن‌ها را می‌بریم، حساس بودیم و رفتن به مکان‌هایی را که مزایای اجتماعی یا رشدی فراهم می‌کردند، در اولویت قرار می‌دادیم. می‌خواهم آن‌ها را به موزه علوم ببرم، اگرچه ترجیح می‌دهم، در تابستان، زمانی که میزان ابتلا در جامعه کمتر بود، از آن جا بازدید کنم.

– چگونه باید اوقات بازی را برای کودکان واکسینه شده یا واکسینه نشده تنظیم کنیم؟

جنیفر نوزو: ایمن‌ترین زمان بازی، اوقاتی است که با سایر بچه‌های واکسینه شده‌ای که فرزندان شما از قبل با آن‌ها در ارتباط بوده‌اند، مانند همکلاسی‌ها بازی کنند. پیش از این که فرزندانم واکسینه شوند، بازی در فضای باز را ترجیح می‌دادم. البته ما هنوز زیر بار بازی در محیط‌های سرپوشیده نرفته‌ایم، اما اکنون که تمام خانواده ما واکسینه شده‌اند و با توجه به اهمیت بازی برای رشد و تکامل کودکان، عموماً احساس راحتی می‌کنم که این کار را انجام دهم.

هوتز: این جا در بخش جنوبی کشور، معمولاً آب و هوا، برای بچه‌ها به اندازهٔ خوب است که در فضای باز بازی کنند یا اگر در داخل خانه هستند، در پشتی یا پنجره را برای تهویه باز بگذارند، در غیر این صورت، من با جنیفر موافقم.

– فرزندان من واکسینه شده‌اند، اما امیدواریم که جشن تعطیلات کوچکی با اعضای خانواده مسن‌تر یا دارای نقص ایمنی داشته باشیم. آیا باید در این باره تجدید نظر کنیم؟

جنیفر نوزو: با توجه به این که همه واکسینه شده اند، امکان تجمع نسبتاً ایمن وجود دارد. آزمایش‌های سریع و استفاده از ماسک، لایه‌های حفاظتی را اضافه می‌کنند. در نهایت، تصمیم باید با اعضای خانواده باشد که در معرض خطر هستند. آن ها باید تصمیم بگیرند که چه سطحی از خطرات اضافی را برای جمع کردن خانواده تحمل می‌کنند.

هوتز: من فکر می‌کنم این بستگی به سطح خطر اساسی، بر اساس سن یا میزان نقص ایمنی افراد دارد. همچنین بستگی به این دارد که مستعدترین افراد در گروه شما برای بیماری، چه زمانی داروهای تقویتی خود را دریافت کرده‌اند، زیرا مطالعات اخیر نشان می‌دهد که محافظت در برابر بیماری با علائم می‌تواند چند ماه پس از دریافت داروهای تقویتی کاهش یابد.

– در گردهمایی‌های بزرگ خانوادگی، چطور ؟

هوتز: هر چه تعداد افراد در یک گردهمایی بیشتر باشد، معمولاً این خطر بیشتر است. من این کار را در طول موج همه‌گیری اومیکرون منع می‌کنم. اما اگر قرار است جمع شوید، توصیه می‌کنم همه کاملا

واکسینه شده و تقویت شوند و مردم از آزمایشات سریع و ماسک استفاده کنند و با باز کردن پنجره‌ها تهویه هوا را افزایش دهند.

– در خانوادهٔ من، کودکانی هستند که برای واکسینه شدن بسیار کم سن و سالند و ما قصد نداریم تغییرات اساسی در اقدامات احتیاطی که تاکنون انجام داده‌ایم، ایجاد کنیم. ما بچه‌هایمان را با ماسک به مدرسه می‌فرستیم و در مراسم کلیسا از ماسک استفاده می‌کنیم. زمانی که فردی علائمی داشته باشد، آزمایشات سریع انجام می‌دهیم. ما قصد داریم در کریسمس از خانواده دیدن کنیم، از جمله دو پدربزرگ و مادربزرگ بالای 70 سال. آیا ما احمق هستیم؟

جنیفر نوزو: من می دانم که عده‌ای اساساً رفتارهای خود را در پاسخ به موارد فزایندهٔ ابتلا تغییر می‌دهند، زیرا نمی‌خواهند به افزایش انتقال یا فشار بر سامانهٔ سلامت کمک کنند. من به شدت از این تلاش‌ها قدردانی و حمایت می‌کنم، اما در جایگاه پدر و مادر، پس از نزدیک به دو سال که بچه‌هایمان را در خانه، بیرون از مدرسه، دور از اقوام در تعطیلات و غیره نگه می‌داریم، انجام این کار واقعاً سخت است.

بنابراین، من فکر می‌کنم پاسخ واقعی‌تر این است که کاری که باید انجام دهید بستگی به تحمل خطر، توانایی شما در ایمن‌تر کردن فعالیت‌ها و توانایی شما برای مقابله با بیماری در صورت ابتلا دارد. آن چه شما توضیح دادید به طور کلی نحوهٔ زندگی خانوادهٔ ما قبل از واکسینه شدن فرزندانمان است. ما رفتن به مکان‌ها و انجام کارهایی را که برای ما در جایگاهِ یک خانواده مهم بود، در اولویت قرار دادیم. برای نمونه، دیدار با خانواده و دوستان نزدیک و رفتن به مدرسه...

البته اومیکرون، اساسا در این که ما چگونه از خود محافظت کنیم، تغییری ایجاد نمی‌کند، اما با توجه به افزایش سطح ابتلا در جوامع، این احتمال را که شما و اعضای خانواده‌تان در معرض ویروس قرار بگیرید، افزایش می‌دهد. با این حال، اقداماتی که ما برای محافظت از خود در برابر این ویروس انجام می دهیم، یکسان است.

من هنوز فکر می‌کنم که می‌توان با اعضای ایمن خانواده دیدار کرد، به خصوص اگر همه کسانی که می‌توانند، واکسینه شوند. آزمایش‌های سریع، درست پیش از دیدار با افرادی که مدتی است ندیده اید، می‌توانند کمک کنند.

تهویهٔ مناسب و ماسک به ایمنی بیشتر این گردهمایی‌ها کمک می‌کنند. حتی اگر خطرات کم باشد، مردم باید برای این واقعیت آماده باشند که ممکن است مبتلا شوند و در صورت ابتلا مجبور به پذیرفتن قرنطینه شوند.

هوتز: ضروری است که همه از واکسن‌های خود نهایت استفاده را داشته باشند. افرادی که واجد شرایط برای استفاده از مواد و داروهای تقویتی هستند باید آن‌ها را دریافت کنند. با توجه به نرخ بالای ابتلای مجدد به بیماری اومیکرون، کسانی که قبلاً آلوده شده بودند، باید واکسینه شوند. همه کودکان پنج سال، بالاتر باید واکسینه شوند.



ژاکلین اشنایدر
پژوهشگر در دانشگاه استانفورد

دنیای بی‌اعتماد
تهدید سایبری موذیانه

منبع فارین افیرز، برگزیدهٔ مقالات نیوزویک، با عنوان انتخاب سردبیر



وقتی زنگ خطر دربارۀ تهدیدهای سایبری به صدا در می‌آید، سیاستگذاران و تحلیلگران معمولاً از واژگانی مانند درگیری و فاجعه استفاده می‌کنند. در اوایل سال ۲۰۰۱، جیمز آدامز، یکی از بنیانگذاران شرکت امنیت سایبری iDefense، در همین نشریه هشدار داد که فضای سایبری «میدان نبرد بین المللی تازه‌ای» است وپیروزی یا شکست در کارزارهای نظامی آینده، در آن‌ها رقم خواهد خورد. در سال‌های بعد، مقام‌های دفاعی ایالات متحده دربارۀ «پرل هاربر سایبری» به قول لئون پانتا، وزیر دفاع وقت و «یازده سپتامبر سایبری» به گفتۀ جانت ناپولیتانو، مشاور امنیت ملی وقت هشدار دادند. در سال ۲۰۱۵، جیمز کلاپر، مدیر وقت اطلاعات ملی گفت: ایالات متحده باید برای «آرماگدون سایبری» آماده شود، اما اذعان کرد که محتمل‌ترین سناریو نیست. در پاسخ به این تهدید، مقام‌های رسمی استدلال کردند که فضای سایبری را باید به سان «گستره‌ای» برای درگیری با «جبهه‌ای کلیدی» برای بهره‌برداری یا دفاع ایالات متحده از آن در نظر گرفت.

بیست سال پس از هشدار آدامز نشان داده است که تهدیدات سایبری و حملات سایبری بسیار نزدیک است- اما نه به آن شکل که اغلب پیش‌بینی کرده‌اند. جاسوسی و دزدی در فضای مجازی حجم سنگینی از اطلاعات حساس و اختصاصی را از بین برده است. عملیات اطلاعاتی سایبری، ادوارانتخاباتی متعددی را در معرض تهدید قرار داده، جنبش های اجتماعی توده‌ای گوناگونی را تحریک کرده است. حملات سایبری به مشاغل مختلف، صدها میلیارد دلار هزینه در پی داشته است، اما در حالی که تهدید سایبری، واقعی و در حال رشد است، انتظار می رود که این گونه حملات آثار عینی وسیعی در مقیاس بزرگی حتی در حد ویرانی‌های ناشی از بمباران‌های غافلگیرکننده در خاک ایالات متحده بر جای بگذارد، یا این که ایالت ها را به درگیری خشونت آمیز سوق دهد، یا حتی آن چه در گسترۀ فضای سایبری رخ داده است، ای بسا مشخص کند چه کسی در میدان جنگ پیروز شده یا شکست خورده است. سیاست گذاران در جریان تلاش برای تشبیه تهدید سایبری به دنیای جنگ عینی، خطر بسیار موذیانه‌تری را که عملیات سایبری ایجاد می‌کند، از دست داده‌اند؛ این که این گونه عملیات، چگونه اعتماد مردم را به بازارها، دولت ها و حتی قدرت ملی، از بین می‌برند.

تشخیص صحیح تهدید، تا حدی به این دلیل ضروری است که روش سرمایه گذاری دولت ها را برای ایجاد امنیت سایبری تعیین می‌کند. تمرکز بر رویدادهای جداگانه و بالقوه فاجعه‌بار و تفکر بیشتر در مورد آثار عینی احتمالی حملات سایبری،

قابلیت‌های پاسداری در برابر «بزرگ‌ترین» خطرها را اولویت‌بندی می‌کند: پاسخ‌های گسترده به حملات سایبری فاجعه‌بار، اقدامات توهین‌آمیز که منجر به خشونت عینی می‌شوند، یا فقط اعمال مجازات برای حملات گوناگونی که مرزبندی‌های راهبردی و استراتژیک را پشت سر بگذارند. قابلیت‌ها و پاسخ‌هایی در این حد، عمدتاً برای حفاظت از اعتماد عمومی به اقتصادها، جوامع، دولت‌ها و ارتش‌های مدرن در برابر حملات سایبری بی‌اثر هستند.

اگر این اعتماد است که در معرض خطر است- پیش از این هم به شدت بی‌رنگ شده- پس گام‌هایی که دولت‌ها برای بقا و فعالیت در این دنیای جدید باید بردارند، متفاوت خواهد بود. راه حل «پرل هاربر سایبری» این است که تمام تلاش خود را انجام دهیم تا اطمینان حاصل کنیم که این اتفاق نمی‌افتد، اما راه حفظ اعتماد در دنیای دیجیتال، با وجود اجتناب ناپذیری حملات سایبری، ایجاد انعطاف پذیری و در نتیجه ارتقای اعتماد به سیستم‌های امروزی اعم از تجارت، حکومت‌داری، قدرت نظامی و همکاری بین المللی است. دولت‌ها می‌توانند این انعطاف‌پذیری را با بازگرداندن پیوندهای انسانی و درون شبکه‌ای، با فعال کردن استراتژیک سیستم‌های آنالوگ در صورت نیاز و با سرمایه‌گذاری در فرآیندهایی که امکان مداخله دستی و انسانی را فراهم می‌کنند، توسعه دهند. کلید موفقیت در فضای سایبری در درازمدت، یافتن راهی برای شکست همه حملات سایبری نیست، بلکه یادگیری نحوۀ حفظ بقا با وجود اختلالات و ویرانی‌هایی است که آن‌ها ایجاد می‌کنند.

ایالات متحده تاکنون «۱۱ سپتامبر سایبری» را تجربه نکرده است و حمله سایبری که آثار عینی فاجعه بار فوری ایجاد کند، در آینده نیز محتمل نیست؛ اما اعتماد آمریکایی ها به دولت، نهادها و حتی هموطنانشان به سرعت در حال کاهش است و این بنیان‌های جامعه را تضعیف می‌کند. حملات سایبری این نقاط ضعف را جذب می‌کند، بی اعتمادی به اطلاعات و سردرگمی و اضطراب ایجاد کند و نفرت و شایعات را گسترش می‌دهد. همان طور که وابستگی‌های دیجیتالی مردم رشد می‌کند و پیوندهای بین فناوری‌ها، افراد و مؤسسات ضعیف‌تر می‌شود، این تهدید سایبری برای اعتماد فقط حیاتی‌تر می‌شود. این آینده دیستوپیایی (کابوس‌آبادی، در برابر مدینۀ فاضله) خزنده است که سیاستگذاران باید نگران آن باشند و هر کاری که ممکن است برای جلوگیری از آن انجام دهند.

گسترش سوء ظن

تمام اعتمادی که برای انجام این تعاملات و مبادلات آنلاین لازم است، یک هدف عظیم ایجاد می کند. به دراماتیک ترین شکل، عملیات سایبری باعث ایجاد بی‌اعتمادی در نحوه عمل سیستم می‌شود و یا پرسش را درست می‌کند که آیا سیستم اصولاعمل می کند؟ مثلا، یک اکسپلویت، یعنی حمله‌ای سایبری که از نقص‌های امنیتی سامانه‌های رایانه‌ای بهره می‌برد، می‌تواند دستگاه ضربان ساز را هک و کنترل کند و باعث بی‌اعتمادی بیمار استفاده کننده از آن شود. یا یک درب پشتی ریزتراشه می‌تواند به بازیگران بد اجازه دهد به سلاح‌های هوشمند دسترسی پیدا کنند و در مورد این که چه کسی کنترل آن سلاح‌ها را در دست دارد، بی‌اعتمادی ایجاد می‌کند. عملیات سایبری می‌تواند منجر به بی‌اعتمادی به یکپارچگی داده‌ها یا الگوریتم‌هایی شود که داده‌ها را معنا می‌کنند؛ آیا گزارش‌های رای دهندگان دقیق هستند؟ آیا سیستم هشدار راهبردی مجهز به هوش مصنوعی، پرتاب واقعی موشک را نشان می‌دهد یا این یک نقطه ضعف در کد رایانه است؟ علاوه بر این، فعالیت در دنیای دیجیتال می‌تواند باعث بی‌اعتمادی در مالکیت یا کنترل اطلاعات شود؛ آیا عکس‌های شما خصوصی مانده‌اند؟ آیا مالکیت معنوی شرکت شما امن است؟ آیا اسرار دولتی دربارۀ سلاح های هسته‌ای به دست دشمنان رسیده است؟ در نهایت، عملیات سایبری با دستکاری شبکه‌ها و روابط اجتماعی و در نهایت کاهش سرمایه اجتماعی، بی‌اعتمادی ایجاد می‌کند. شخصیت‌های آنلاین، ربات‌ها و کمپین‌های اطلاعات نادرست، همگی این موضوع را پیچیده می‌کنند که آیا افراد می‌توانند هم به اطلاعات و هم به یکدیگر اعتماد کنند. همه این تهدیدات سایبری پیامدهایی دارند که می‌توانند بنیان‌ها و ارکانی را که بازارها، جوامع، دولت‌ها و نظام بین‌الملل بر آن ساخته شده‌اند، از بین ببرند.

اقتصاد وابسته به دیجیتال به ویژه در برابر تخریب

اعتماد آسیب پذیر است. همان طور که بازار مدرن به صورت آنلاین به هم پیوسته‌تر شده است، تهدیدات سایبری پیچیده‌ترشده‌اند و همه جا حضور دارند. برآوردهای سالانه هزینه کل اقتصادی حملات سایبری از صدها میلیارد تا تریلیون دلار متغیر است، اما تنها هزینه مالی این حملات نیست که اقتصاد مدرن را تهدید می کند، بلکه چگونگی بروز بی اعتمادی دربارهٔ یکپارچگی سیستم، تحت تاثیر این حملات پی در پی، به عنوان یک کل مزید بر علت است.

چنین چیزی، هیچ جا، به اندازه واکنش مردم به حملهٔ باج افزار به خط لولهٔ انتقالی نفت آمریکا مشهود نبود. در ماه مه ۲۰۲۱، یک باند جنایتکار به نام DarkSide این خط لوله را که حدود ۴۵ درصد سوخت را به سواحل شرقی ایالات متحده می‌رساند، تعطیل کرد و باج خواست که در نهایت شرکت پرداخت کرد. به رغم تأثیر محدود این حمله بر توانایی شرکت در تأمین نفت مشتریانش، مردم وحشت زده، با مخازن نفت و کیسه‌های پلاستیکی برای ذخیره بنزین به پمپ بنزین‌ها هجوم آوردند که منجر به کمبود مصنوعی شد. این نوع بی‌اعتمادی و هرج و مرج ناشی از آن، نه تنها بنیان‌های اقتصاد دیجیتال، بلکه کل اقتصاد را نیز تهدید می‌کند.

ناتوانی در محافظت از مالکیت معنوی در برابر سرقت سایبری نیز به همین ترتیب مشکل زودهنگامی است. عمل سرقت مالکیت معنوی یا اسرار تجاری از طریق هک کردن شبکهٔ شرکتی معین و گرفتن داده‌های حساس، به تجارت جنایی پرسودی تبدیل شده است؛ اقدامی که کشورهایی از جمله چین و کره شمالی از آن برای رقابت با ایالات متحده و دیگر کشورهایی که دارای خلاقانه‌ترین فن‌آوری‌ها هستند به آن دست می‌یازند. کره شمالی در تلاش برای سرقت فن‌آوری واکسن کووید-۱۹، شرکت داروسازی فایزر را هک کرد و نفوذ چینی‌ها در تحقیقات پایگاه صنعتی دفاعی ایالات متحده منجر به کپی برداری از پیشرفت‌های فن‌آورانهٔ توسعه هواپیما و موشک شده است. هرقدر چنین حملاتی گسترده‌تر و پیچیده تر شوند، شرکت‌ها کمتر می‌توانند اعتماد کنند که سرمایه گذاری آن‌ها در تحقیق و توسعه منجر به سود خواهد شد و در نهایت اقتصادهای دانش بنیاد را نابود خواهد کرد و هیچ جا تهدیدی برای اعتماد بیشتر از بانکداری آنلاین وجود ندارد. اگر کاربران دیگر اعتماد نداشته باشند که داده‌های دیجیتال و پولشان قابل محافظت است، کل سیستم مالی مدرن پیچیده ممکن است سقوط کند. بدتر، چرخش به سمت ارزهای رمزنگاری شده، که بیشترشان از تضمین‌های دولتی برخوردار نیستند، اعتماد به ارزش اطلاعات دیجیتال را بیش از پیش حیاتی می‌کند.

جوامع و دولت‌ها نیز در برابر حملات اعتماد آسیب پذیر هستند. مدارس، دادگاه‌ها و دولت‌های شهری همگی به اهداف باج‌افزاری تبدیل شده‌اند که باعث می‌شوند سیستم‌ها آفلاین گردند یا تا زمانی که قربانی هزینه را پرداخت نکند، بی‌استفاده می‌شوند. در دل این شبکه‌ای در هم تنیده، کلاس‌های درس مجازی، دسترسی به سوابق قضایی و خدمات اورژانس محلی وجود دارد. در حالی که تأثیر فوری این حملات می‌تواند به طور موقت، برخی از عملکردهای حکومتی و اجتماعی را کاهش دهد، خطر بزرگتر این است که در درازمدت، بی‌اعتمادی به یکپارچگی داده‌های ذخیره شدهٔ دولت‌ها- اعم از



سوابق ازدواج، گواهی تولد، سوابق جنایی، یا تقسیم اموال- می‌توانند اعتماد به کارکردهای اساسی جوامع را از بین ببرد. اتکای دموکراسی به اطلاعات و سرمایه اجتماعی برای ایجاد اعتماد در موسسات به طور قابل ملاحظه‌ای در برابر عملیات اطلاعاتی سایبری آسیب پذیر است. کمپین‌های حمایت شده از سوی دولت که پرسش‌هایی را دربارهٔ یکپارچگی داده‌های حکومت‌داری (مانند شمارش آرا) برمی‌انگیزد، یا جوامع را به گروه‌های کوچکی تقسیم می‌کند که به منابع خاصی اعتماد دارند، نیروهایی را به وجود می آورد که ناآرامی های مدنی را دامن می‌زنند و دموکراسی را تهدید می‌کنند.

عملیات سایبری همچنین می‌توانند با حمله به اعتماد به سلاحهای مدرن، قدرت نظامی را به خطر بیندازد. با ظهور قابلیت‌های دیجیتال، با شروع ریزپردازنده، دولت‌ها شروع به تکیه بر سلاح‌های هوشمند، حسگرهای شبکه‌ای و پلت‌فرم‌های مستقل برای ارتش‌هایشان کردند. از آن جایی که این ارتش‌ها از نظر دیجیتالی توانمندتر شده‌اند، در مقابل، عملیات سایبری که قابلیت اطمینان و عملکرد این سیستم‌های تسلیحاتی هوشمند را تهدید می‌کرد، هم حساس شده‌اند. در حالی که تمرکز قبلی روی تهدیدات سایبری بر این بود که چگونه عملیات سایبری می‌تواند مانند یک بمب عمل کند، خطر واقعی، زمانی رخ می‌دهد که حملات سایبری، اعتماد به این که بمب‌های واقعی آن‌طور که انتظار می‌رود کار می‌کنند، کاهش دهند. همان طور که نظامیان با انجام عملیات از راه دور، از میدان نبرد دورتر می‌شوند و فرماندهان مسئولیت را به سیستم های خودمختار محول می‌کنند، این اعتماد بیش از پیش مهم می‌شود. آیا ارتش‌ها می‌توانند باور داشته باشند که حملات سایبری، سیستم‌های خودمختارشان را از کار نمی‌اندازد، یا حتی بدتر، باعث برادرکشی یا کشتن غیرنظامیان نمی‌شود؟ علاوه بر این، برای ارتش‌های بسیار شبکه‌ای (مانند ارتش ایالات متحده)، درس‌های گرفته شده از عصر اطلاعات اولیه، منجر به آموزه‌ها، کمپین‌ها و سلاح‌هایی شده که بر توزیع‌های پیچیدهٔ اطلاعات تکیه دارند. بی‌اعتمادی به اطلاعات یا وسایلی که از طریقشان منتشر می شود، باعث زمین‌گیر شدن ارتش‌ها خواهد شد، چون در انتظار دستورات جدید می‌مانند و مطمئن نیستند که چگونه باید ادامه دهند. این عوامل در کنار هم، سیستم‌های شکنندهٔ اعتمادی را که سبب تقویت صلح و ثبات در نظام بین المللی می‌شود، تهدید می‌کنند، امکان تجارت را کاهش می‌دهند، کنترل تسلیحات را دشوارتر می‌کنند و دولت‌ها را دربارهٔ نیات یکدیگر نامطمئن‌تر می‌کنند. معرفی ابزارهای سایبری برای جاسوسی، حملات و سرقت، تنها آثار بی‌اعتمادی را تشدید کرده است. نظارت بر قابلیت‌های سایبری تهاجمی دشوار است و فقدان هنجارهایی برای استفادهٔ مناسب از عملیات سایبری، اعتماد دولت‌ها را به پایبندی دیگران به محدودیت‌های وضع شده، دشوار می‌سازد. آیا هکرهای روسی در حال کاوش در شبکه‌های قدرت ایالات متحده برای انجام حملات سایبری قریب الوقوع هستند یا صرفاً در حال بررسی نقاط آسیب پذیر هستند و هیچ برنامه‌ای برای استفاده از آن‌ها در آینده ندارند؟ آیا عملیات سایبری «پیش دستی در دفاع» ایالات متحده، واقعاً برای جلوگیری از حملات احتمالی به شبکه‌های ایالات متحده است یا برعکس، پوشش برای توجیه حملات سایبری

تهاجمی به سیستم‌های فرماندهی و کنترل چین یا روسیه؟ در همین حال، استفاده از مزدوران، واسطه‌ها و عملیات‌های منطقه خاکستری در فضای مجازی، انتساب و تعیین قصد را سخت‌تر می‌کند و اعتماد و همکاری را در نظام بین‌الملل بیشتر تهدید می‌کند. برای نمونه، نرم افزارهای جاسوسی اسرائیل که به تلاش‌های دولت عربستان سعودی برای سرکوب مخالفان کمک می‌کند، هکتویست‌های نظامی چینی خارج از وظیفه، سازمان‌های جنایی که دولت روسیه به آن‌ها اجازهٔ فعالیت می‌دهد، اما رسما از آن‌ها حمایت نمی‌کند، همه این‌ها، ایجاد، زنجیرهٔ مشخص از انتساب برای یک اقدام عمدی دولتی را دشوار می کند. چنین واسطه‌هایی همچنین سودمندی توافق‌های رسمی بین دولت‌ها درباره رفتار مناسب در فضای مجازی را تهدید می‌کنند.

زندگی با شکست

تا به امروز، راه‌حل‌های ایالات متحده برای خطرات موجود در فضای سایبری، بر بخش فضای سایبری این پرسش متمرکز بوده است؛ بازدارندگی، دفاع در برابر و شکست دادن تهدیدات سایبری هنگام حمله به اهداف خود. اما این استراتژی‌های متمرکز سایبری با مشکل مواجه شده و حتی شکست خورده‌اند. چون حملات سایبری در حال افزایش است، کارایی بازدارندگی مشکوک است و رویکردهای تهاجمی نمی‌توانند موج حملات در مقیاس کوچک را که بنیادهای مدرن و دیجیتالی جهان را تهدید می‌کنند، مهار کنند. سوء استفاده‌های عظیم، مانند هک‌های اخیر نرم‌افزار مدیریت شبکه SolarWinds و نرم‌افزار ایمیل مایکروسافت اکسچنج سرور، کمتر از آن که نشانه‌ای برای شکست دفاع سایبری ایالات متحده باشد، نشانه‌ای از آن است که سیستم‌های هدف قرار گرفته، در گام نخست، چگونه طراحی و ساخته شده‌اند. هدف نباید متوقف کردن همه نفوذهای سایبری، بلکه باید ساختن سیستم‌هایی باشد که قادر به مقاومت در برابر حملات دریافتی هستند. این درس جدیدی نیست. هنگامی که صدای غرش توپ و باروت در قرن چهاردهم و پانزدهم در اروپا شنیده شد، شهرها برای زنده ماندن از هجوم نیروی آتش جدید به دست و پا افتادند. در این راستا، دولت‌ها استحکاماتشان را تطبیق دادند، خندق‌ها حفر کردند، سنگرها ساختند، سواره نظام سازمان‌دادند، بناهای چند ضلعی گسترده ساختند؛ همه با این فکر که شهرهایی را بسازند که بتوانند از محاصره جان سالم به در ببرند، نه این که مانع از اصابت گلولهٔ توپ شوند. بهترین استحکامات برای توانمندسازی دفاع فعال طراحی شده بود و تا زمانی که با ضد حمله‌ای توفنده بتوانند نیروهای باقی ماندهٔ خارج از شهر را شکست دهند، مهاجمان را زمین‌گیر می‌کرد.

این مقایسه، ایجاد استراتژی سایبری مشابهی را طلب می‌کند که در آن تمرکز بر خود سیستم است، خواه سلاح هوشمندی باشد، یا شبکه‌ای الکتریکی و خواه ذهن رأی دهنده‌ای آمریکایی. چگونه می‌توان سیستم‌هایی ساخت که بتوانند در دنیایی از اعتماد ضعیف به کار خود ادامه دهند؟ در این جا، نظریهٔ شبکه - مطالعه چگونگی موفقیت، شکست و بقای شبکه‌ها - راهنمایی‌هایی ارائه می‌دهد. مطالعات روی استحکام شبکه نشان می‌دهد که قوی‌ترین شبکه‌ها آن‌هایی هستند که تراکم بالایی از گره‌های کوچک و مسیرهای متعدد بین گره‌ها دارند. شبکه‌های بسیار انعطاف‌پذیر می‌توانند در برابر حذف گره‌ها و پیوندهای متعدد بدون تجزیه مقاومت کنند، در حالی که شبکه‌های متمرکز و کمتر انعطاف‌پذیر، با مسیرهای کمی و گره‌های پراکنده‌تر، آستانه بحرانی بسیار پایین‌تری برای تخریب و شکست دارند. اگر اقتصادها، جوامع، دولت‌ها و نظام بین‌الملل بخواهند از فرسایش جدی اعتماد عمومی، جان سالم به در ببرند، به بندها و پیوندهای بیشتر، وابستگی کمتر به گره‌های مرکزی و راه‌های جدید برای بازسازی اجزای شبکه، حتی زمانی که تحت حمله هستند نیاز خواهند داشت. این ویژگی‌ها با هم به اعتماد عمومی در یکپارچگی سیستم‌ها منجر می‌شود. چگونه دولت‌ها می‌توانند چنین شبکه‌هایی بسازند؟



- اگر کاربران دیگر اعتماد نداشته باشند که می توان از داده ها و پول آنها محافظت کرد، سیستم مالی مدرن ممکن است سقوط کند.

اول، در سطح فنی، شبکه‌ها و ساختارهای داده‌ای که زیربنای اقتصاد، زیرساخت‌های حیاتی و قدرت نظامی هستند، باید تاب‌آوری را در اولویت قرار داد. این به شبکه‌های غیرمتمرکز و متراکم، ساختارهای ابری ترکیبی، برنامه‌های کاربردی اضافی و فرآیندهای پشتیبان نیاز دارد. این امر، مستلزم برنامه‌ریزی و آموزش برای شکست شبکه است تا افراد بتوانند حتی در بحبوحه یک کمپین سایبری توهین‌آمیز، سازگار شوند و به ارائه خدمات ادامه دهند. این به معنای تکیه بر پشتیبان‌گیری فیزیکی برای مهم‌ترین داده‌ها (مانند آراء) و گزینه‌های دستی برای سیستم‌های عامل، درست در زمانی است که قابلیت‌های دیجیتال در دسترس نیست. برای برخی از سیستم‌های بسیار حساس (برای نمونه، فرماندهی و کنترل هسته‌ای) ممکن است گزینه‌های آنالوگ، حتی زمانی که کارایی کمتری دارند، انعطاف پذیری قابل توجهی ایجاد کنند. کاربران باید اطمینان داشته باشند که قابلیت‌ها و شبکه‌های دیجیتال به گونه‌ای طراحی شده‌اند که به جای شکست فاجعه‌آمیز، به خوبی کاهش سطح می‌دهند: تمایز بین اعتماد دوتایی (یعنی اعتماد به سیستم کاملاً فعال است، یا اصلاً به سیستم اعتماد نمی‌کند) و تداوم اعتماد (اعتماد به عملکرد سیستم در درصدی بین صفر تا ۱۰۰ درصد) باید طراحی قابلیت‌ها و شبکه‌های دیجیتال را هدایت کند. این انتخاب‌های طراحی نه تنها اعتماد کاربران را افزایش می‌دهد، بلکه انگیزه‌های بازیگران جنایتکار و وابسته به دولت‌ها را برای انجام حملات سایبری کاهش می‌دهد.

انعطاف پذیری زیرساخت های حیاتی و قدرت نظامی در برابر حملات سایبری، آثار مثبتی بر ثبات بین المللی خواهد داشت. زیرساخت‌ها و جمعیت‌های انعطاف‌پذیرتر، کمتر در معرض تأثیرات سیستمیک و بلند مدت حملات سایبری هستند، زیرا می‌توانند به سرعت بازگردند. این انعطاف پذیری، به نوبه خود، انگیزهٔ دولت‌ها برای حمله پیشگیرانه به یک دشمن را به صورت آنلاین کاهش می‌دهد، زیرا آن‌ها کارآمدی حملات سایبری و تواناییشان برای وادار کردن جمعیت هدف را زیر سوال می‌برند. متجاوزان، در مواجهه با حمله‌ای دشوار، پرهزینه و بالقوه بی‌اثر، کمتر احتمال دارد که در وهله اول، فواید افزایش حملات سایبری را ببینند. علاوه بر این، کشورهایی که بر ایجاد انعطاف‌پذیری و پایداری در نیروهای نظامی مجهز به امکانات دیجیتالشان تمرکز می‌کنند، کمتر احتمال دارد دست به ضربهٔ اولیه یا عملیات تهاجمی، مانند حملات موشکی دوربرد یا یورش‌های پیشگیرانه بزنند. معضل امنیتی- زمانی که کشورهای بی‌علاقه به جنگ ضد یکدیگر، ناگهان به سبب بی‌اعتمادی به نیات یکدیگر، خود را در تنش می‌بینند- نشان می دهد که وقتی دولت‌ها بیشتر بر دفاع تمرکز می کنند تا حمله، کمتر به سمت درگیری‌هایی می‌روند که در تنش‌های ناشی از بی‌اعتمادی و دودلی می‌روند.

منابع انسانی

با این حال، حل و فصل جنبه‌های فنی، تنها بخشی از راه حل است. مهمترین روابط اعتمادی که فضای مجازی تهدید می‌کند، شبکه‌های انسانی جامعه است - یعنی بندها و پیوندهایی که مردم، خواه تک تک افراد باشند و خواه در جایگاه همسایه و شهروند، دارند تا بتوانند با هم برای حل مشکلات همکاری کنند. راه حل‌هایی برای دوام بیشتر این شبکه‌های انسانی حتی پیچیده‌تر و دشوارتر از هر اصلاح فنی است. رشته عملیات اطلاعات سایبری، پیوندهایی را هدف قرار می‌دهند که بین مردم و جوامع اعتماد ایجاد می‌کنند. آن‌ها این ارتباطات گسترده‌تر را با ایجاد انگیزه برای تشکیل شبکه‌های خوشه‌ای از اعتماد خاص تضعیف می‌کنند؛ برای مثال، پلت فرم‌های رسانه‌های اجتماعی که گروه‌هایی از افراد همفکر را سازماندهی می‌کنند یا کمپین‌های اطلاعات نادرست که تقسیمات درون گروهی و برون گروهی را ترویج می‌کنند. الگوریتم‌ها و طعمه‌های کلیکی که برای ترویج خشم طراحی شده‌اند، فقط این



تقسیم‌بندی‌ها را تقویت می‌کنند و اعتماد افراد خارج از گروه را کاهش می‌دهند. دولت‌ها می‌توانند سعی کنند این نیروها را در رسانه‌های اجتماعی تنظیم کنند، اما این مناطق مجازی منعکس‌کننده شکاف‌های واقعی در جامعه هستند. و یک حلقه بازخورد وجود دارد: بی‌اعتمادی که در فضای آنلاین ایجاد می‌شود به دنیای واقعی نشت و افراد را بیشتر به گروه‌هایی از «ما» و «آن‌ها» جدا می‌کند. مبارزه با این امر مستلزم آموزش و مشارکت مدنی است- لیگ‌های بولینگ که پاتنم می‌گفت برای بازسازی سرمایه اجتماعی آمریکایی‌ها ضروری است (کتاب پاتنم «بولینگ تک نفره»)، به طور اتفاقی، در سال ۲۰۰۰ منتشر شد، یعنی درست زمانی که اینترنت شروع به رشد کرد). پس از دو سال از یک بیماری همه گیر جهانی و انشعاب بیشتر آمریکایی‌ها در مناطق تحت محاصره مجازی، زمان آن فرا رسیده است که جوامع عینی را نیرویی دوباره دهیم، زمان آن فرا رسیده است که محله‌ها، مناطق مدرسه و شهرها گرد هم آیند تا بندها و پیوندهایی را که برای نجات جان انسان ها در طول این مدت قطع شده بودند، بازسازی کنند. همه گیری واقعیت این است که این تقسیم‌بندی‌ها در جوامع آمریکایی حتی قبل از اینکه همه‌گیری یا اینترنت تثبیت آن‌ها را تسریع و قدرت آنها را تقویت کند، در حال تشدید بود. بنابراین راه حل، راه انجام این نوع بازسازی، از رسانه های اجتماعی، مدیران عامل آن پلتفرم ها یا ابزارهای دیجیتال نخواهد بود. در عوض، به رهبران محلی شجاعی نیاز است که می توانند اعتماد را از پایه بازسازی کنند و راه هایی برای گرد هم آوردن جوامعی که از هم جدا شده اند بیابند. قطع ارتباط با اینترنت و گروه‌های ترکیبی اعتماد ویژه‌ای که در آنجا شکل گرفته‌اند، به منظور اتصال مجدد شخصاً نیاز خواهد داشت. آموزش مدنی می‌تواند با یادآوری اشتراکات و اهداف مشترک به جوامع کمک کند و با ایجاد متفکرانی انتقادی که می‌توانند برای تغییر در نهادهای دموکراتیک تلاش کنند.

بولینگ با هم

ضرب‌المثلی وجود دارد که می‌گوید عملیات‌های سایبری با هزاران بریدگی منجر به مرگ می‌شوند، اما شاید شبیه‌تر آن موریانه‌هایی باشند که در خلل و فرج بنیان‌های جامعه پنهان شده‌اند و به تدریج ساختارهایی را که برای حمایت از زندگی مردم طراحی شده‌اند، از درون می‌خورند. تمرکز استراتژیک قبلی روی عملیات سایبری یک باره و در مقیاس بزرگ منجر به امکانات سایبری بزرگ‌تر و بهتری شده است، اما هرگز به شکنندگی درون بنیادها و شبکه‌ها توجهی نشد.

آیا حملات سایبری هرگز باعث آن نوع آثار فیزیکی جدی خواهد شد که در دو دهه گذشته از آن بیم داشتیم؟ آیا راهبردی که بیشتر بر اعتماد و انعطاف‌پذیری

متمرکز باشد، دولت‌ها را به طور منحصر به فردی در برابر این آسیب‌پذیری قرار می‌دهد؟ البته غیرممکن است که بگوییم هیچ حمله سایبری، هیچ گاه آثار عینی وسیعی، در ابعاد مشابه به آثار ناشی از بمباران پرل هاربر ایجاد نخواهد کرد. با این حال، بعید به نظر می‌رسد؛ زیرا ماهیت فضای مجازی، شخصیت مجازی، گذرا و دائماً در حال تغییر، ایجاد آثار عینی پایدار را برای انجام حملاتی ضدش دشوار می کند. استراتژی‌هایی که با سرمایه گذاری در شبکه‌ها و روابط بر اعتماد و انعطاف پذیری تمرکز می کنند، این نوع حملات را دشوارتر می‌کنند. بنابراین، تمرکز بر ساخت شبکه‌هایی که می‌توانند از حملات بی‌وقفه و کوچک‌تر جان سالم به در ببرند، یک محصول جانبی اتفاقی دارد؛ انعطاف‌پذیری بیشتر در برابر حملات یک باره و در مقیاس بزرگ.

اما چنین چیزی آسان نیست و استراتژی‌هایی که به منظور نیل به راحتی یا بازدارندگی و شکست تهدیدات سایبری، انعطاف‌پذیری، افزونگی و پشتکار را اساس فعالیت خود قرار می‌دهند، باید تا اندازهٔ قابل توجهی، میان کارایی و هزینه تعادل و موازنه ایجاد کنند و طبیعی است که هزینه اولیهٔ اقداماتی که برای تقویت اعتماد عمومی صورت می‌پذیرد، به طور نامتناسبی، بر دوش دموکراسی‌ها بیفتد. چون باید برخلاف اتکای ویژه‌ای که حکومت‌های استبدادی به قدرت دارند، مجبورند اعتماد عمومی را پرورش دهند. چنین اقدامی مانند بلعیدن داروی تلخ و بدمزه‌ای است، آن هم در شرایطی که به نظر می‌رسد چین و ایالات متحده به طور فزاینده‌ای پا به رقابت تنگاتنگی نهاده‌اند.

با وجود مشکلات و هزینه‌ها، دموکراسی‌ها و اقتصادهای مدرن (مانند ایالات متحده) باید اعتمادسازی به سیستم‌هایی را که جوامع را اداره می‌کنند- اعم از شبکه برق، بانک‌ها، مدارس، ماشین‌های رأی‌گیری یا رسانه‌ها- در اولویت قرار دهند. چنین اقدامی به معنای اجرای برنامه‌های پشتیبان‌ساز (بک آپ) و ایمن‌ساز failsafe تصمیم‌گیری استراتژیک در مورد اینکه چه چیزی باید آنلاین یا دیجیتال باشد و چه چیزی باید آنالوگ یا فیزیکی باقی بماند و ساخت شبکه‌هایی - چه آنلاین و چه در جامعه - که می‌توانند حتی زمانی که یک گره در معرض حمله قرار می‌گیرد، زنده بمانند. اگر رمز عبور سرقت شده همچنان بتواند خط لوله نفت را از بین ببرد، یا یک حساب کاربری جعلی در شبکه های اجتماعی بتواند نظرات سیاسی هزاران رای دهنده را تحت تاثیر قرار دهد، در این صورت حملات سایبری برای نظام‌های استبدادی و جنایتکاران بسیار سودآور خواهد بود. ناکامی در ایجاد انعطاف پذیری بیشتر- چه فنی و چه انسانی- به این معنی است که چرخه حملات سایبری و بی اعتمادی ناشی از آن‌ها همچنان ارکان جامعه دموکراتیک را تهدید می‌کند.



آنتونی فیولا

در ترکیه، منتقدان می‌گویند که سلطان لباس ندارد. مشاوران اردوغان به او نمی‌گویند.

منبع: واشنگتن پست

در ترکیه لیر در حال سقوط است و آسمان هم همین طور! قیمت‌ها در سوپرمارکت‌ها تقریباً هر روز در حال تغییر است. خطوط تولید نان یارانه‌ای در حال افزایش است. ترک‌ها قادر به تامین هزینه‌های سیب زمینی، آرد و مرغ نیستند. تقریباً همهٔ کارشناسان، یک مرد را مقصر می دانند: رئیس جمهور رجب طیب اردوغان!

اردوغان مستبد که در اولین دورهٔ ریاست جمهوری جورج دبلیو بوش به قدرت رسید، عملاً به بازار مالی سنتی اعلان جنگ داده است و با کاهش نرخ بهره، به خرمن بحران ارزی آتش می زند. در حالی که اقتصاددانان استدلال می کنند که او باید دقیقاً برعکس عمل کند و برای دفاع از ارزش لیر، از این بازار حمایت کند.

اما اردوغان که ادعا می کند اقتصاد خوانده است، می‌گوید که او بهتر از همه می‌داند. او با درخواست از ترک‌ها برای «صبور» بودن، اصرار دارد که ارز ضعیف‌تر و نرخ‌های بهره پایین‌تر، صادرات ترکیه را تقویت می‌کند، شغل ایجاد می‌کند، رشد را تحریک می‌کند و تورم را کاهش می‌دهد. اقتصاددانان می گویند: آن چه او از ذکر آن غفلت می‌ورزد این است که چنین سیاستی، به ویژه در شرایط بحرانی، باعث افزایش قیمت کالاهای اساسی نیز می‌شود، سرمایه گذاران خارجی را می‌ترساند، بانک‌های ترکیه را خالی می‌کند و با افزایش تورم، مردم را فقیر می‌کند. روز پنجشنبه، کاهش جدید نرخ بهره که چهارمین کاهش در چهار ماه گذشته بود، باعث شد لیر به پایین ترین سطح خود سقوط کند. در روز جمعه، سرمایه گذاران سر از پا نمی‌شناختند و در میان عملیات سر سام آور فروش ارز، سقوط آزاد ارزش، باعث شد مدار شکن های بازار سهام ظرف یک ساعت، دو بار متوقف شود.

منتقدان می‌گویند که اردوغان با انباشتن قدرت در دستانش، در طول سالیان متمادی و نیز با حذف کسانی که او را زیر سئوال می‌بردند، اکنون در احاطه افراد «بله قربان گو» قرار گرفته است. او آزاداندیشان بانک مرکزی ترکیه را اخراج کرده است و کارشناسان را نگران کرده است که ممکن است کسی در اطراف رئیس جمهور نباشد که به گوش او برساند سلطان لخت است. در حالی که لیر به نزول خود ادامه می دهد و تاکنون، نیمی از ارزشش را در برابر دلار در سال جاری از دست داده است، ترک‌های فقیر و متوسط حال، بالاترین قیمت را می‌پردازند، زیرا قیمت کالاهای اصلی دو برابر شده و هزینه سوخت تا چهل درصد افزایش یافته است.

یکی از فروشندگان خیابانی آنکارا به نیویورک تایمز گفت: «فکر می‌کنم پایان دنیا نزدیک است».

تحلیلگران شروع به این سوال کرده‌اند که آیا حماقت‌های مالی اردوغان ممکن است کاری را به جایی برساند که سال‌ها تحکیم قدرت و شیوه‌های سرکوبگرانه انجام نداده‌اند و در نهایت، به قیمت مشاغل مردم تمام شود؟

سینان اولگن، کارشناس ترک در کارنگی اروپا، به من گفت: «به نظر می‌رسد او واقعاً معتقد است که درست می‌گوید، در حالی که بقیه دنیا برعکس آن را درست می‌دانند». اگر این سیاست شکست بخورد، او همچنان محبوبیت خود را از دست خواهد داد. در حال حاضر، دیگر رقبای ریاست جمهوری در نظرسنجی ها پیروز شده اند.»

شرط بندی علیه اردوغان اغلب با شکست مواجه می شود. در طول دو دهه گذشته، او بارها و بارها موفق شده است که ناملایمات را به پیروزی تبدیل کند. با موفقیت در بحران‌های ژئوپلیتیکی، کودتای مبهم و بهار ترکیه، تقریباً همیشه قوی‌تر ظاهر می‌شود و در عین حال حمایت محافظه‌کاران اسلامی را در قلب حزب عدالت و توسعهٔ تحت امر خود حفظ کرده است. اگر همان طور که اپوزیسیون تاکید کرده است، انتخابات زودهنگام برگزار نشود – احتمالی که اردوغان رد کرده است – انتخابات ریاست جمهوری بعدی تا سال ۲۰۲۳ برگزار نخواهد شد.

با این حال، بحران‌های اقتصادی می‌توانند به سیاستمداران خیانت کنند. فقط از آرژانتینی ها بپرسید که چگونه در بحبوحه سقوط ویرانگر ارز و بحران بدهی در اواخر سال ۲۰۰۱، پنج رئیس جمهور را در دو هفته کنار گذاشتند. کار ترکیه هنوز به آن جا نرسیده و به دلایلی از جمله بدهی‌های خارجی

قابل مدیریت، احتمالاً از فروپاشی به سبک آرژانتینی جلوگیری خواهد شد. با این حال، رهبران خودکامه‌ای مانند اردوغان بارها در میان هرج و مرج اقتصادی سقوط کرده‌اند. در سال ۲۰۱۹، عمر حسن البشیر، رئیس‌جمهور سودان، پس از رشته تظاهراتی که در واکنش به افزایش هزینه‌های مواد غذایی و سوخت آغاز شد، با یک کودتای نظامی از قدرت برکنار شد. برخی از کارشناسان قیمت بالای مواد غذایی را یکی از عوامل بهار عربی می‌دانند. برای باقی ماندن در قدرت، خودکامگان تمایل دارند خودکامه‌تر شوند. در ونزوئلا، رئیس جمهور نیکلاس مادورو – از متحدان نزدیک اردوغان - با وجودِ تورم سنگین و بحران انسانی وحشتناک ناشی از آن، با نزدیکتر کردن کشور به دیکتاتوری کامل، جان سالم به در برده است.

اگرچه اردوغان اکنون در جامعهٔ خودکامگی دیده می‌شود، اما هنوز پا در این راه نگذاشته است. او در سال ۲۰۰۳ گفت: «من موافق این دیدگاه نیستم که فرهنگ اسلامی و دموکراسی را نمی‌توان با هم آشتی داد.» سال‌های اولیه ریاست جمهوری اردوغان باعث شد تا او یک نهاد نظامی فعال از جمله تعداد زیادی سرباز و افسر فعال و بازنشسته را رام کند. سیاست‌های طرفدار سرمایه‌گذاری او در ابتدا باعث رونق اقتصادی شد که نرخ فقر را کاهش داد و زیرساخت‌های جدید پیشرفته‌ای را به شهرهای ترکیه آورد.

برخی نقطه بازگشت او را به خودکامگی، سال ۲۰۱۳ می‌دانند، زمانی که او از واکنش خشونت آمیز به اعتراضات پارک گزی در استانبول حمایت کرد که در آغاز، در مخالفت با توسعه شهری آغاز شد، اما به اعتراض عمومی گسترده‌تری ضد آزادی‌های رو به زوال تبدیل شد.

در سال ۲۰۱۸، اردوغان برای تغییر سیستم پارلمانی به سیستمی ریاستی، با رئیس جمهوری نیرومند تلاش کرد و پیروز شد، شغلی که اکنون دارد و در آن، آزادی بیشتری برای دور زدن پارلمان دارد. اما حتی قبل از آن، در کسوتِ نخست وزیر، با مهار مطبوعات، مخالفان را خفه کرده بود. او پس از کودتای ۲۰۱۶ ارتش را هم پاکسازی کرد.

با این حال، از سال ۲۰۱۸، ترکیه نیز از یک محاسبه دردناک اقتصادی جلوگیری کرده است. لیر سقوط کرد، زیرا اردوغان به دنبال رشد اقتصادی به هر قیمتی است و کاهش نرخ بهره را راهی برای دستیابی به آن می‌بینند. مشکلات جاری در ماه مارس شتاب گرفت، زمانی که اردوغان که به دنبال کاهش بیشتر نرخ بهره بود، سومین رئیس بانک مرکزی خود را در کمتر از دو سال برکنار کرد و ساهاپ کاوچی اوغلو را جایگزین او کرد.

استیون اِی کوک در فارین پالیسی نوشت: «شرایط اصلی رئیس بانک مرکزی جدید برای تصدی این وزارتخانه، صرفا پیوندهایش با داماد رئیس جمهور، یعنی برات آلبایراک است که دوران تصدی وی در کسوتِ وزیر دارایی و خزانه داری فاجعه بار بود».

اردوغان از مواضع خود دفاع کرده و با استناد به تحریم‌های اسلامی ضد نرخ بهرهٔ بالا، به چین به سانِ نمونه‌ای اشاره می‌کند که چگونه نرخ‌های بهره پایین و ارز ضعیف‌تر می‌توانند طبقه متوسط رو به رشدی ایجاد کنند.

اما این امر زمان‌بر خواهد بود – چیزی که ترکیه ممکن است با توجه به سقوط سریع لیر که هزینه‌های تولید در داخل را نیز افزایش داده است، فاقد آن باشد. ترکیه برای بسیاری از صادرات نهایی خود – مانند خودرو – قطعات وارد می کند که با توجه به لیر ضعیف، اکنون خرید آن‌ها گران‌تر است.

در این میان، مشکلات ارزی باعث تعمیق نارضایتی‌ها و تحریک اعتراضات ضد دولتی می‌شود. این هفته، وال استریت ژورنال گزارش داد؛ MAK – یک شرکت مشاوره سیاسی طرفدار دولت – گفت که محبوبیتِ حزب عدالت و توسعه در نظرسنجی‌ها، برای اولین بار به زیر سی درصد رسیده است.

گزارش وال استریت ژورنال، از شهر ریزه، زادگاه رئیس جمهور، این احساسات تلخ را به تصویر کشید. چیزی که باید مایهٔ نگرانی اردوغان باشد.

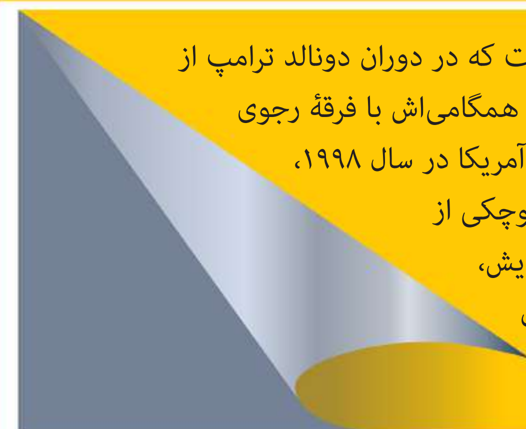
مهمت علیباریس، یک چای‌کار در نزدیکی شهر ریزه که از شدت تورم ورشکست شده است، به ژورنال گفت: « ما ته چاهیم. ما هیچ قدرت خریدی نداریم. من به هر کسی که ما را از شر این دولت خلاص کند، رای خواهم داد.»

پیش به‌سوی شکست فاجعه‌بار آمریکا

نیوت گینگریچ

منبع: نشریهٔ نیوز ویک

ایالات متحده به‌سوی شکستی فاجعه‌بار پیش می‌تازد.



نیوت گینگریچ که اکنون در سمت مشاور سیاسی فعالیت دارد و اندیشکده‌های سیاسی متعددی را تاسیس کرده است، جمهوری‌خواهی فوق‌العاده تندروست که در دوران دونالد ترامپ از حامیان اصلی‌اش بود. بسیاری از کارشناسان، او را در کنار امثال جان بولتون، نمایندهٔ جریانی تندرو در راست سنتی می‌دانند. موضع‌گیری‌های او ضد ایران و همگامی‌اش با فرقهٔ رجوی موسوم به مجاهدین خلق و گرفتن مبالغ سنگینی پول از آن‌ها بر کسی پوشیده نیست. او در کل، سیاستمدار فاسدی است و استعفایش از مجلس نمایندگان آمریکا در سال ۱۹۹۸، در حاشیهٔ یکی از همین بداخلاقی‌هایش روی داد. او این روزها، آتش‌بیار معرکه‌ای با چین شده است. مقالهٔ او که در نشریهٔ نیوزویک منتشر شده، نمونهٔ کوچکی از تلاش‌های سیاست بازان آمریکایی برای ایجاد موج تازه‌ای در عرصهٔ سیاستگزاری آمریکاست. معلوم نیست که نیوت گینگریچ، این بار در استخدام کارفرماهایش، قصد دارد چه کار کند؟ شاید تلاشی برای افزایش سرمایه‌گذاری دولت در حوزهٔ خریدهای تسلیحاتی از شرکت‌های بزرگ جنگ‌افزارسازی آمریکا، با دامن زدن به خطر چین و بزرگ‌نمایی در این زمینه..!

من در مورد شکستی صحبت می کنم که آزادی ما را از بین می‌برد و آمریکا را برای همیشه تابع چین کمونیست و خواسته‌هایش درراستای کنترل و فرمانبری مطلقمان خواهد کرد.

ممکن است فکر کنید این دیدگاه هشداردهنده است، اما کافی است به کنترل حزب کمونیست چین بر هنگ کنگ، سوءاستفاده‌هایش در تبت و نسل کشی اویغورها در سین کیانگ نگاه کنید.

برای این موضوع، به شرکت‌های غول‌پیکر و ثروتمند آمریکایی نگاه کنید که از پیش، به خواسته‌های حزب کمونیست چین سر تعظیم فرود می‌آورند و زبان و رفتارشان را برای آرام کردن پکن هماهنگ می‌کنند.

پس از فشار چین، دیزنی به دلیل اشاره به قتل عام میدان تیان آن من در سال ۱۹۸۹، قسمتی از سریال «سیمپسون‌ها» را از سرویس پخش خود در هنگ کنگ حذف کرد. نایک و کوکاکولا، در مخالفت با قانون ممنوعیت واردات کالاهای ساخته شده با کار اجباری در چین لابی کردند. جی‌پی مورگان چیس، با وجودِ خطرات جدی امنیت داده‌ها و امنیت ملی، تجارتش را در چین گسترش داده است و به خاطر دارد، وقتی داریل موری، مدیر کل هیوستون راکتس، حمایت خود را از دموکراسی در هنگ کنگ توئیت کرد، چه قشقرقی به پا شد؟ NBA و بازیکنان ریز و درشتش، برای عذرخواهی بی‌شرمانه در حمایت از سانسور در چین صف کشیدند. واقعا چندش‌آور بود!

برخی از میلیاردرهای آمریکایی با همکاری چین کمونیست آن قدر پول به دست آورده‌اند که منافع جیب خود را بر ارزش‌های آمریکایی و منافع امنیت ملی آمریکا اولویت تام داده‌اند.

آمریکای شکست خورده، تابع دیکتاتوری کمونیست چین خواهد بود. سخنان، رفتارها و نهادهای ما دائماً برای راضی کردن دیکتاتوری بیماران سوظن دائم در پکن تنظیم می‌شود.

با وجودِ پیامدهای فوق العاده شکست، نظام امنیتی آمریکا به تدریج به سمت و سوی نوعی نظام امنیت ملی کشانده می‌شود که در نهایت، به شکست آشکاری در جنگ بزرگ با چین کمونیست تن خواهد داد.

حرف من را قبول نکنید!

اما فرماندهان رده بالای ارتش آمریکا ناقوس خطر را

به صدا درآورده‌اند.

همان طور که Epoch Times در این ماه گزارش داد، ژنرال دیوید تامپسون، ژنرال نیروی فضایی ایالات متحده هشدار داد که «اگر آمریکا روند توسعه خود را شتاب نبخشد، چین می‌تواند تا سال ۲۰۳۰ از نظر قابلیت های فضایی از ایالات متحده پیشی بگیرد.»

این نشریه افزود: «واقعیت این است که در اصل، به طور متوسط، [چین] در حال ساخت و میدان دادن و به روزرسانی قابلیت‌های فضایی [خود] با سرعتی دو برابر ما است.»

با وجود این تهدید فزاینده در فضا، زمانی که معاون رئیس جمهور کامالا هریس ریاست اولین جلسه شورای ملی فضایی دولت را در این ماه بر عهده داشت، حتی یک موضوع نظامی هم مورد بحث قرار نگرفت.

فراتر از افزایش آسیب‌پذیری در فضا، با وجود این که ژنرال‌ها گزارش داده‌اند که روسیه و چین تقریباً هر روز با ایالات متحده در فضا درگیر می‌شوند، ما همچنین، در توانایی‌های دفاعیمان هم با بحرانی عمومی رو به رو هستیم.

Business Insider در این باره می‌نویسد: «ارتش ایالات متحده پس از «شکست سختی» در بازی جنگی‌اش در برابر دشمن متجاوزی که قواعد بازی خود را می‌دانست، نحوه مبارزه‌اش را تغییر می‌دهد.»

جو بایدن، رئیس جمهور ایالات متحده، در ۱۵ نوامبر ۲۰۲۱، در نشستی مجازی از اتاق روزولت کاخ سفید در واشنگتن دی سی، با شی جین پینگ، رئیس جمهور چین، ، ملاقات کرد. ماندل نگان/ خبرگزاری فرانسه از طریق GETTY IMAGES.

معاون رئیس ستاد مشترک ارتش، ژنرال جان هایتن در کنفرانسی در ماه ژوئیه هشدار داد: «بدون اغراق در این موضوع، او به طرز بدی شکست خورد.»

هایتن توضیح داد: در این بازی جنگی که درگیری با چین را بر سر تایوان شبیه‌سازی می‌کرد، ما درگیر دشمنی بودیم که درگیری‌ها و جنگ‌های آمریکا را برای دو دهۀ تمام مطالعه کرده بود. همان طور که او می‌گفت، چین فرضی « فقط دور ما زنگ می زد. آن‌ها دقیقاً می‌دانستند که ما قرار است چه کاری انجام دهیم و از آن سوء استفاده می‌کردند.»

هایتن هشدار داد که چین کمونیست واقعی به طور مشابه استراتژی‌های نظامی ما را «با تمرکز بیشتر، با تعداد بیشتر» مطالعه کرده است. همان طور که او بیان کرد، ما باید تغییرات جدی ایجاد کنیم، زیرا توانایی ما برای رقابت با قدرت‌های رقیب از جمله چین «به سرعت در حال کاهش است.»

دریاسالارانی که تعهدات نظامی آمریکا را در اقیانوس آرام برعهده دارند نیز ، در بارۀ شکست سیستم‌های فعلی ما سخن گفته‌اند.

به گزارش گاردین، دریاسالار بازنشسته فیلیپ دیویدسون که بیست و پنجمین فرمانده ستاد فرماندهی هند و اقیانوسیۀ ایالات متحده بود، در ماه مارس گفت: «جنگ جدی بر سر تایوان، ممکن است در شش سال آینده رخ دهد.»

دیویدسون گفت: «من نگران هستم که [چین] به جاه طلبی‌های [خود] برای جانشینی ایالات متحده و دستیابی به نقش رهبری ما در نظم بین المللی تا سال ۲۰۵۰ جامۀ تحقق بپوشاند.»

هنگامی که دریاسالار چهار ستاره بازنشسته جیمز استاوریدیس در ماه ژوئن، درباره رمان جدیدش، ۲۰۳۴ رمانی دربارۀ جنگ جهانی بعدی، با روزنامۀ ژاپنی آساهی شیمبون مصاحبه کرد، او این احساس را دربارۀ توانایی‌های رو به رشد چین تقویت کرد:

« زمانی که شروع به نوشتن رمان کردم، این جنگ بزرگ، در اواسط قرن، تقریباً سال ۲۰۵۰ اتفاق می‌افتد؛ اما هر چه بیشتر تحقیق می‌کردم و تحلیل‌هایم را در بارۀ وضع موجود بیشتر به کار می‌گرفتم، تاریخ نزدیک‌تر می‌شد. بسیاری از دوستانم، افسران بسیار ارشد ارتش، اعم از فعال و بازنشسته، و سیاستگذاران ارشد، از این کتاب ستایش کرده‌اند؛ با این حال، آن‌ها به من گفتند: «تو رمانی عالی نوشتی، اما یک اشتباه بزرگ داشتی و آن تاریخ است.» بسیاری بر این باورند که تاریخ رویارویی آمریکا و چین زودتر خواهد بود.

به عنوان آخرین نمونه از آسیب پذیری آمریکایی، جیمز کیتفیلد در ماه مارس دربارۀ درگیری شبیه سازی شده بسیار محرمانه‌ای با چین که با استفاده از تسلیحات بیولوژیکی چین آغاز شد، مطلبی در بخش خبری یاهو نوشت. این نبرد، با تهاجم گسترده‌ای که در پوشش مانوری معمولی پنهان شده بود، ادامه یافت و با حملات موشکی ویرانگر ضد پایگاه‌ها و کشتی‌های جنگی هند و اقیانوس آرام و همچنین خود تایوان به اوج رسید.

نیازی به گفتن نیست که آمریکا این نبرد مجازی را هم از دست داد. قانون مجوز دفاع ملی فعلی، خیلی ساده، به میزان تغییراتی که ما به منظور اطمینان از توانایی آمریکا برای شکست نظامی چین، نیاز داریم، نمی‌پردازد.

پنتاگون و جامعه اطلاعاتی ، با حواس پرتی تمام، ت وجه خود را به آماده باش نیروی‌ها و نه تشکیل نیروی‌های قادر به پیروزی درجنگ معطوف کرده‌اند و این، آمریکا را بیشتر تضعیف می کند.

ما به پژوهشی دربارۀ ضروریات و بایستگی‌های پیروزی نظامی بر چین و نیز تعهدی برای انجام هرگونه اصلاحاتی در سیستم دفاعی، آموزش، بازارهای سرمایه، زنجیره‌های تدارکاتی، تولید صنعتی و دیگر حوزه‌ها، به منظور تضمین امنیت و آزادی آمریکا نیاز مبرم داریم.

هر اقدامی جز بازنگری کامل در \ توانایی‌هایمان و تغییر روند تلاش‌های سیستماتیک و سازمند حزب کمونیست چین برای تبدیل شدن به ابرقدرت مسلط بر جهان، ممکن است به شکست ما، در زمانی بسیار کوتاه‌تر از آن چه فکر می‌کنید، منجر شود.

آزادی و امنیت ما هر دو در خطر است.

این باید به اصلی اساسی برای سال های ۲۰۲۲ و ۲۰۲۴ تبدیل شود.

نظرات بیان شده در این مقاله مربوط به خود نویسنده است.

Oriental Voice 1



winter 22